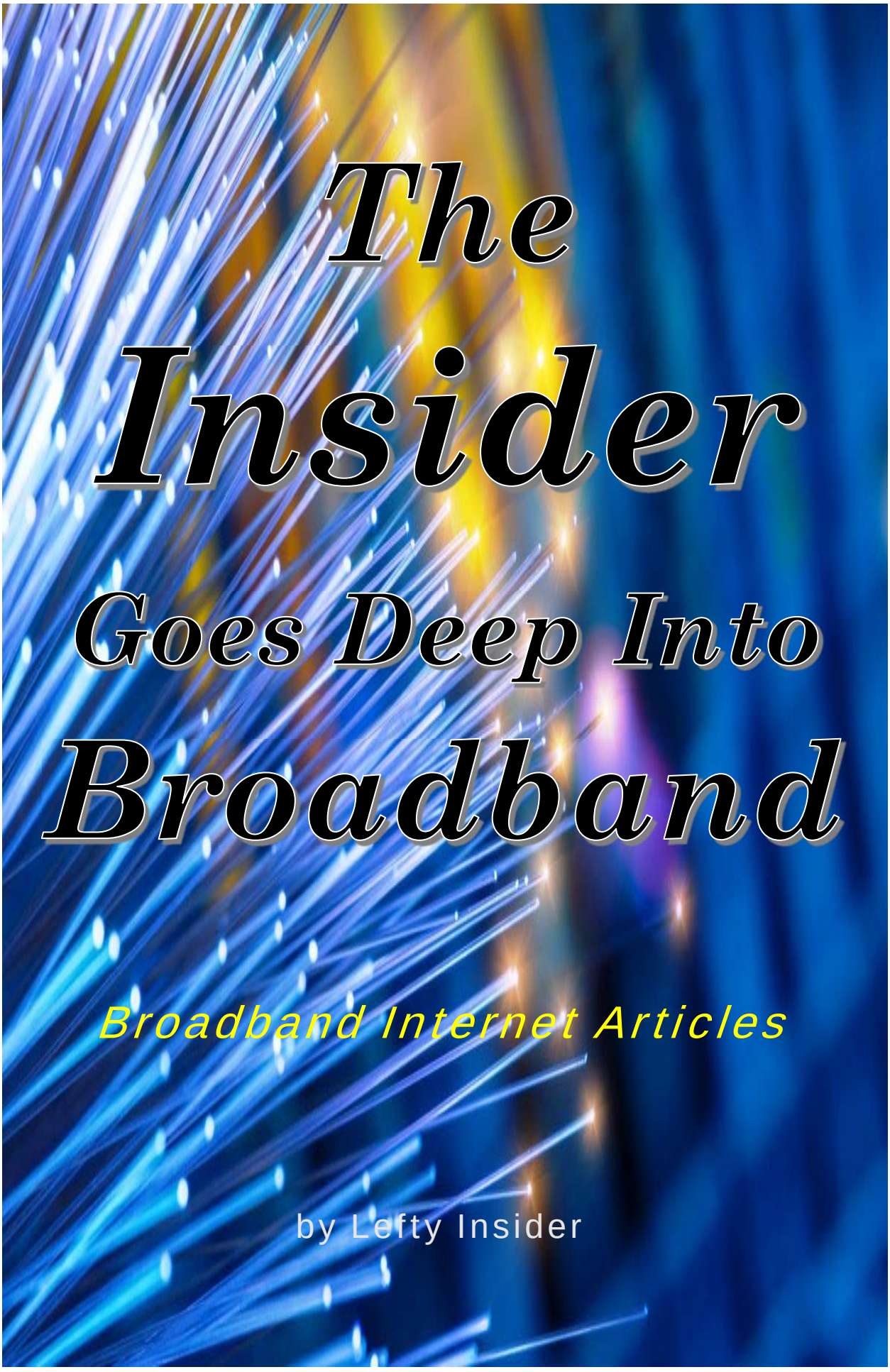
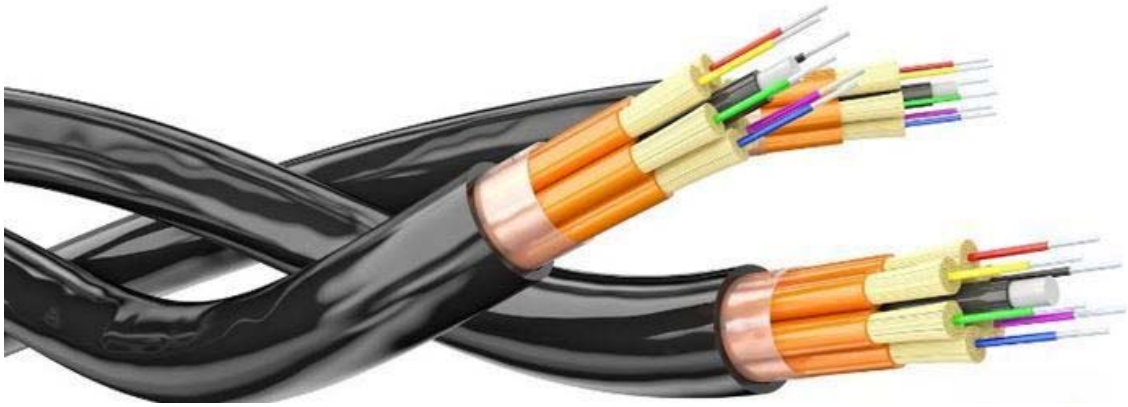

The
Insider
Goes Deep Into
Broadband
Broadband Internet Articles
by Lefty Insider

About the Title

The Insider Goes Deep into Broadband (Broadband Internet Articles) title is a collection originally published individually on Medium.com.

Target Market

This collection is targeted primarily to a demographic of 10 million college educated Baby Boomer aged men who are working in, or have worked in, the IT fields. The proposed goal of this manuscript is to reach one percent of this market, most of whom are disinclined to use social media, and find pdf files more accessible and readable than poorly formatted and weakly illustrated eBooks.



Fiber cables

Acknowledgements

Those involved in the creation of this book, know who they are and are much appreciated by this author.

Editor and publisher
Lefty Insider
Insider Publishing, LLC
Last edited January, 2025

ISBN number 979-8-9922163-6-3

Note: No one's clouds were used to create this book.

Inspirations

About the Author

He was born and raised in Wisconsin. He is a veteran of the US Army U.N. Peace keeping force in South Korea, a former Peace Corps volunteer in West Africa and former Illinois high school and Community College teacher. He holds a BS in Education degree from the University of Illinois-Urbana/Champaign and has completed Master's degree work in Adult Distance Education..

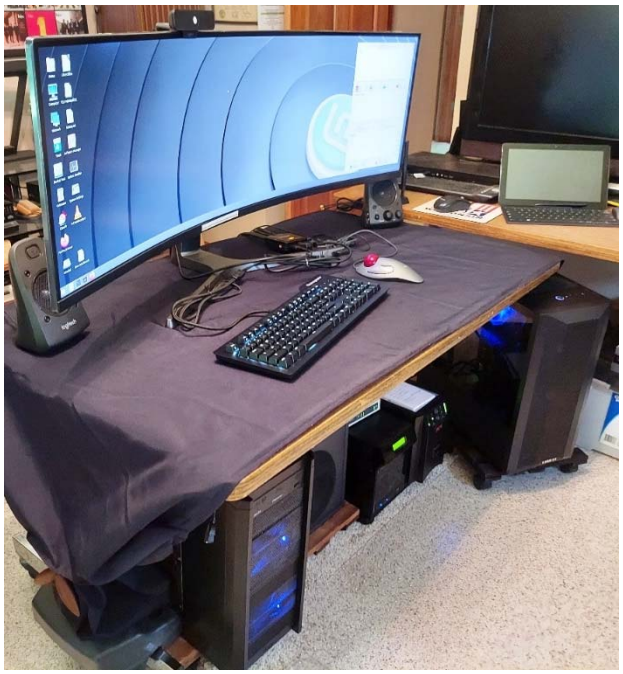
Following and during his teaching positions, he was involved in corporate technical service training and course development for International Harvester and JI Case companies taking him to North Dakota and Illinois.

He then operated a Tri-County business as President/CEO, involved in the sale and support of business computer systems, as well as specially adapted systems for the disabled. He was also the Executive Director and Board President of a statewide non-profit volunteer group dedicated to helping provide children with computer and Internet technology access. They refurbished and delivered many thousands of computer systems and provided Internet service as an ISP. He was also a Microsoft Partner, Microsoft Original Equipment Manufacturer System Builder or OEM, and a Microsoft Registered Refurbisher, or MAR.

He has lived in three countries on three continents and in five states, allowing him to write and publish six novels and a dozen short stories.

Lefty Insider resides in the beautiful farm and forest countryside of Wisconsin with his loving wife. He retired from active work a decade ago but continues to work with computer technology, reading, and challenging himself with new learning and self-directed pursuits.

He writes from his well-equipped home office.



He works in his home office with a window view of his backyard wild turkey farm.

Synopsis

This Insider Goes Deep Into Broadband novella is in many ways is a sequel to the writers' previous Insider books that follows the continued corruption (enshitification)[1] of computer operating systems and software programs in supporting the devolution of the original Internet into an individualized predatory surveillance system, and global societal menace whose parasitic effects, and predatory behavior threaten lives, freedom, and democracy.

Also from this author. The Insider titles are as follows:

Book One
The Insider (A Life Inside the Personal Computer)

Book Two
The Cozening (A Murder of Promise)

Book Three
The Insider Goes Deep (Tales from the Dark Web)

Book Four
A User Guide To The Dark Web (The 42nd and Final Encyclopedia Cyberspacia)
The above is a companion book to Book Three

Book Five
The Insider Goes Deep into the Spectrum
A quest to get the Megabits promised and paid for, "one sweet megabit at a time"

Book Six(TBD)
The Insider Goes to Space (Tales from Beyond Planet Earth)

Book Seven
The Insider Goes Deep into Broadband (Broadband Internet Articles)

Book Eight (TBD)
The Insider Goes Deep into the Legal System (A Journey NOT for the Faint of Heart)

Book Nine (TBD)
The Insider Goes Deep into the Consumer Protection System (It's Worse Than You Think)

Note: All released books are available on leanpub.com
https://leanpub.com/bookstore?type=all&search=lefty%20insider

[1] *Cory Doctorow https://en.wikipedia.org/wiki/Enshittification*

A Note to Readers:

Throughout this book and the previous prequels, this writer chooses to write the term Internet with its original and intended initial capitalization spelling as a proper noun. This is also true for any outside imported text. The Internet is a person, place, or thing and as we were all taught in grade school, requires proper capitalization. The trend in current print and online spelling as *lower case, which* is disrespectful to its founders and creators in my view.

It is this writer's view that this intentional diminishment, via the lower case spelling, of this technological wonder and gift to humanity, is part of an effort by Corporate America to assimilate it into their Corporate Borg. To the founders, decentralization was the main idea, not the current walled gardens of Google (Alphabet), Apple, Amazon, Microsoft, and Facebook (MEA). While original pioneers like Vint Cerf may have been assimilated into the corporate Borg, people like Jon Postel and Tim Berners-Lee never were. Anyway, this writer gets to decide such things.

Note: this book is best read with a pdf reader and not a web browser, in Read Mode, and in portrait orientation, which allows for both page turning and to zoom in on the graphics contained within. A 1600x900 or higher screen resolution on a 24 inch portrait monitor is recommended.

This book and the entire collection represent this writer's lifetime opus in the form of an extended modern day bildungsroman representing more than ten years of writing work and more than fifty years of research and life experience. As with the previous books in this series, this one is part invented fiction, part historical fiction, part textbook, and part actual journalism.

These books are what Americans may call *edgy* or *anti-establishment* and contain what the writers Germans ancestors might call *Sturm und Drang*.[2]

[2] *A late 18th century German literary movement characterized by works containing rousing action and high emotionalism that often deal with the individual's revolt against society*

Dedication

The book is dedicated to the numerous Internet Elders and those who created and developed the Personal Computer.

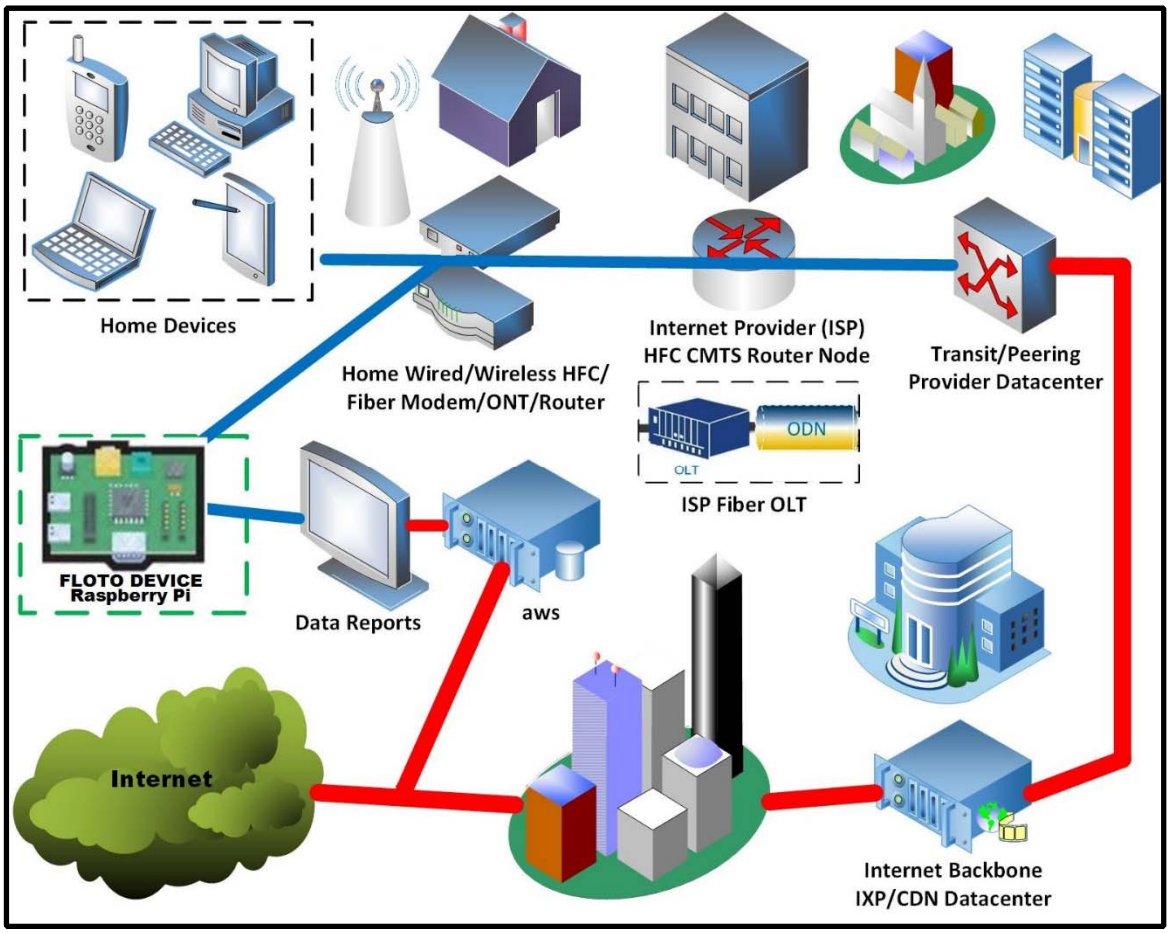
Fair use rationale for illustrations & lyrics

This publication does not limit, nor claim to limit, the rights of the copyright holder. They remain the property and copyright of their owners.

Partial song lyrics are used as descriptive words.

Other graphics are either self-created, public domain via Wikimedia Commons, where attribution is not required, or come from the Creative Commons.

Copyright disclaimer under Section 107 of the Copyright Act of 1976, allowances are made for "Fair Use" for purposes such as criticism, comment, news reporting, teaching, scholarship, and research. Fair Use is a use permitted by copyright statute that might otherwise be infringing. Non-Profit, educational, or personal use tips the balance in favor of Fair Use.



A primitive mapping of a user's view of the Internet as it pertains to them

Table of Contents

An Informed Citizens View of the Current Broadband Fiber Kerfuffle

An Informed Citizens View of the Current Broadband Fiber Kerfuffle (Part Two)

An Informed Citizens View of the Current Broadband Fiber Kerfuffle (Part Three)

An Informed Citizens View of the Current Broadband Availability Kerfuffle

An Informed Citizens View of the Current Broadband Affordability Kerfuffle

An Informed Citizens Report from the Consumer Internet Trenches

An Informed Citizens View of the Current Broadband CyberSecurity Kerfuffle (Part One)

An Informed Citizens View of the Current Broadband CyberSecurity Kerfuffle (Part Two)

An Informed Citizens View of the Current Broadband CyberSecurity Kerfuffle (Part Three)

An Informed Citizens View of the Current Broadband CyberSecurity Kerfuffle (Part Four)

An Informed Citizens View of the Current Broadband CyberSecurity Kerfuffle (Part Five)

An Informed Citizens View of the Current Broadband CyberSecurity Kerfuffle (Part Six)

An Informed Citizens View of the Current Wisconsin Broadband Kerfuffle (Extended)

An Informed Citizens View of the Current Broadband Fiber Kerfuffle

(We all need to reject the whiners, profiteers, naysayers, and just get to work)

Rural broadband Internet in this country for the most part remains monopolized, overpriced, insufficiently fast, hampering economic growth and resilience, as well as educational and healthcare opportunities. Federal government programs are currently funding the BEAD, RDOF and other programs to help alleviate this, but progress is stalled and delayed by federal regulations, corporate interests, and lobbying by wealthy executives who have bought influence in our legislatures. Now the naysayers and the profiteers, smelling government monies, are getting louder and a looming corporate government takeover may either kill, or wound these programs significantly. The US, as creator of the NSFNET/ARPANET/INTERNET, currently ranks 27th in Internet broadband availability and 32nd in affordability, in the developed world. This Internet is no longer a luxury, but a necessity, and these ratings should be a disgrace to us all.

Critics also argue that fiber networks are too expensive and unnecessary, promoting wireless, and satellite alternatives instead. However, these alternatives offer slower speeds far slower than fiber's current and future potential. As Harvard's Professor Crawford writes, it is like comparing our current 2-inch copper water pipes to a 14-mile-wide fiber optic cable river.

While burying fiber may be costly in some areas, existing electrical, telephone, and railroad right-of-ways—often now hiking trails—offer an underused infrastructure that could be repurposed to string aerial or bury fiber cables. The government granted these right of ways, and they can now be reclaimed for the public good, via eminent domain if necessary.

All wireless technologies, cellular, fixed wireless, and satellite suffer from the same issues.

1) Satellite has affordability (hardware and service) as well as connection viability issues
2) They all require subsidizing noncompetitive costs (require 50-75% consumer subsidies)
3) They all have upgrade/maintenance issues High maintenance and upgrade cycles
   -4G, 5G, 6G cellular hotspots, high cost, low performance
   -Multiple upgrades of Starlink in the past five years is detrimental (costly) to consumers
   -Broadband Point-to-Point Wireless (urban and rural) only advanced from 1-100 Mbps over 5 years
4) They all have low performance/high maintenance/upgrade costs, and limited capacity compared to fiber wired line technologies
5) They all require line of sight or near line of site to towers or views of the northern sky (questionable viability in rural hilly and wooded areas)

There is an old computer IT maximum that rings true still today that says that:
"*wired is for data, and wireless is for voice".*

We do have other options using fiber optic based networks, such as:

Open Access Community-owned internet networks versus subsidizing incumbent monopoly ISPs:

These networks provide long-term ROI (Return on Investment) through equal access, local control, and economic growth. Initial costs are high but Open Access community networks recoup investments by avoiding profit-driven ISPs (quarterly Wall Street expectations) to offer affordable pricing. They attract businesses, creating jobs, and support education. They address digital divides by prioritizing underserved areas while remaining accountable to residents, which can result in better service and lower fees and generate long-term revenue that can be reinvested into local infrastructure.

Subsidies to ISPs often result in limited long-term ROI. They reduce immediate costs for consumers, but do not guarantee affordability. Incumbents also fail to serve rural areas without substantial incentive subsidies and do not provide lasting infrastructure assets, leading to higher future costs.

Open Access Community networks need significant upfront investment but offer sustainable equal access stimulants to economic activity without continual funding or addressing systemic inequities.

Open Access Community-owned networks deliver better long-term ROI by creating lasting infrastructure, leased to the incumbent monopolies, promoting economic and digital equity. While subsidies can offer short-term relief, they lack the transformative impact of some of the current 2000 community-owned systems.

The current incumbent monopoly ISP's failed to deliver widespread service and affordability over the past thirty years. It is long past overdue to follow in the footsteps of our ancestors, who brought us nationwide affordable and reliable electricity and telephone networks. Rural citizens were not relegated to second class citizen status with electricity or telephone networks. They did not provide 120 volts of electricity to urban citizens and 60 volts to rural ones. They just did what it took and got it done.

The analogy is clear: just as railroads and telegraphs connected the country in the past, we must now invest in future-proof fiber networks to ensure rural citizens are not left behind. As hockey legend Wayne Gretzky said, *"Skate to where the puck is going, not where it is now."* 10 Gbps and beyond is where this puck is going, and Open Access competitive fiber middle mile networks and Open Access competitive last mile networks are the only reasonable ways to get there. The future is fiber, and it's time we act to meet the progress of previous generations who built our railroads, roads, and communication networks.

It is necessary for us to see beyond a narrow vision and the limitations of self-interest, to see and do the important and the necessary and retouch with our humanity to obtain a view of the greater good.

As humans with the unique, in the animal world, ability of imagination, it is incumbent on us to strive to utilize this gift in a manner to provide the fullest opportunities for the advancement of our civilization and progressive human achievements.

By Michael F. Pitsch, PO Box 322 Francis Creek, WI 54214 November, 25th, 2024

"The use of an instrument so powerful for good or evil, cannot with safety to the people be left in the hands of private individuals uncontrolled by law." Postmaster general Cave Johnson in 1845 speaking of the telegraph but is certainly applicable to the current Internet

Literary Source References:

The Book of Violations & Egregious Acts: Trillion Dollar Broadband Scandal
A summary of 30-years of research, outlining massive incumbent monopoly tax cuts, regulatory provisions, broken promises, and monetary subsidies. http://irregulators.org/egregiousacts/

Electrifying Rural America
During the Great Depression, communities banded together to bring electricity to America's farmland. https://www.richmondfed.org/-/media/richmondfedorg/publications/research/econ_focus/2020/q1/economic_history.pdf

ROI for funding Community Owned Internet Networks vs subsidizing access to incumbent ISPs
When comparing the ROI (Return on Investment) of funding community-owned internet networks versus subsidizing access to incumbent ISPs, several factors come into play. By Dr. Ron Suarez November 20, 2024 https://communityinter.net/roi-for-funding-community-owned-internet-networks-vs-subsidizing-access-to-incumbent-isps/

Provide Universal High-Speed Broadband Internet for All, Dramatically Lower Costs, Break Up and Regulate Internet and Cable Monopolies, Build Resilient Communications Networks
https://berniesanders.com/issues/high-speed-internet-all/

My Plan to Invest in Rural America
A Public Option for Broadband
https://medium.com/@teamwarren/my-plan-to-invest-in-rural-america-94e3a80d88aa

Starlink, the truth is out there: Sam Crawford
https://www.samknows.com/blog/starlink

Fiber: The Coming Tech Revolution—and Why America Might Miss It
Professor Susan Crawford Yale University Press (January 8, 2019)
https://www.allconnect.com/blog/united-states-ranks-27th-in-global-internet-connectivity
https://www.telecompetitor.com/report-u-s-is-32nd-worldwide-on-broadband-affordability/

This is the eleventh in a series of articles on Broadband Internet

An Informed Citizens View of the Current Broadband Fiber Kerfuffle (Part Two)

(Starlink – it's worse than you think, and why would someone even consider tax funding this.)

A Starlink Constellation circling the earth about every 90 minutes or so

All satellite technologies suffer from the same issues.

1) Satellite has affordability (hardware and service) as well as connection viability issues
2) Satellite systems require potentially permanent subsidizing of noncompetitive costs
3) Satellite systems have expensive upgrade/maintenance issues
4) Satellite systems have low performance/high maintenance/upgrade costs, and limited capacity compared to fiber wired line technologies
5) Satellite systems require line of sight or near line of site to views of the northern sky (questionable viability in rural hilly and wooded areas)

Note: this article will focus exclusively on Starlink as most of SpaceX's potential competitors – Amazon's Project Kuiper, One Web, and AST Space Mobile – have yet to launch their full constellations or are still in the early stages of development.

Some Important Facts to Consider

Starlink Sky View Angle

Based on the provided search results, here are the key findings:

1. **Unobstructed view 25 degrees above the horizon**: Starlink requires an unobstructed view 25 degrees above the horizon in **every direction**. This means that the dish needs to be installed in a location where there are no obstructions (trees, buildings, etc.) within a 25-degree cone above the horizon.

2. **100-degree cone centered on the dish's pointing direction**: The dish also needs an unobstructed view within a 100-degree cone centered around its pointing direction after it tilts. This cone is not fixed in azimuth (direction) and varies depending on the location.
3. **Optimum angle for satellite coverage**: Starlink's dish will automatically level itself to search for satellites overhead and tilt to the optimum angle for satellite coverage, which is slightly north or south based on the user's location in the northern or southern hemisphere.

It's essential to note that these requirements are based on the assumption that the dish is installed **as close to vertical as possible**. If a clear field of view cannot be achieved from ground level, installing the dish in an elevated location (e.g., roof, pole, or wall) may be necessary.

For users in heavily obstructed areas, we recommend checking for obstructions with the Starlink app prior to ordering Starlink, to assess your field of view. (www.Starlink.com)

Installation at the northern latitudes (°N) 42.5 - 46.6.

While the dish is heated (unlike DIRECTV) to prevent problems from the buildup of ice and snow, it will also attract some neighborhood *friends* if you do not tower or roof mount it. Of course, this was harder to do in the winter months and people tend to set the dish on the ground.

Bandwidth and latency

Ookla studies show download speeds in the range of the mid-60's Mbps. However, this low result is likely from users using their phones to connect to the less than stellar Starlink wireless router, and like most other Ookla's speed tests, in my view, are marginally accurate for a number of reasons. According to users, Starlink bandwidth also fluctuates wildly during the day, and it directly influenced by the clarity of the sky. (Despite Starlink's claims otherwise)

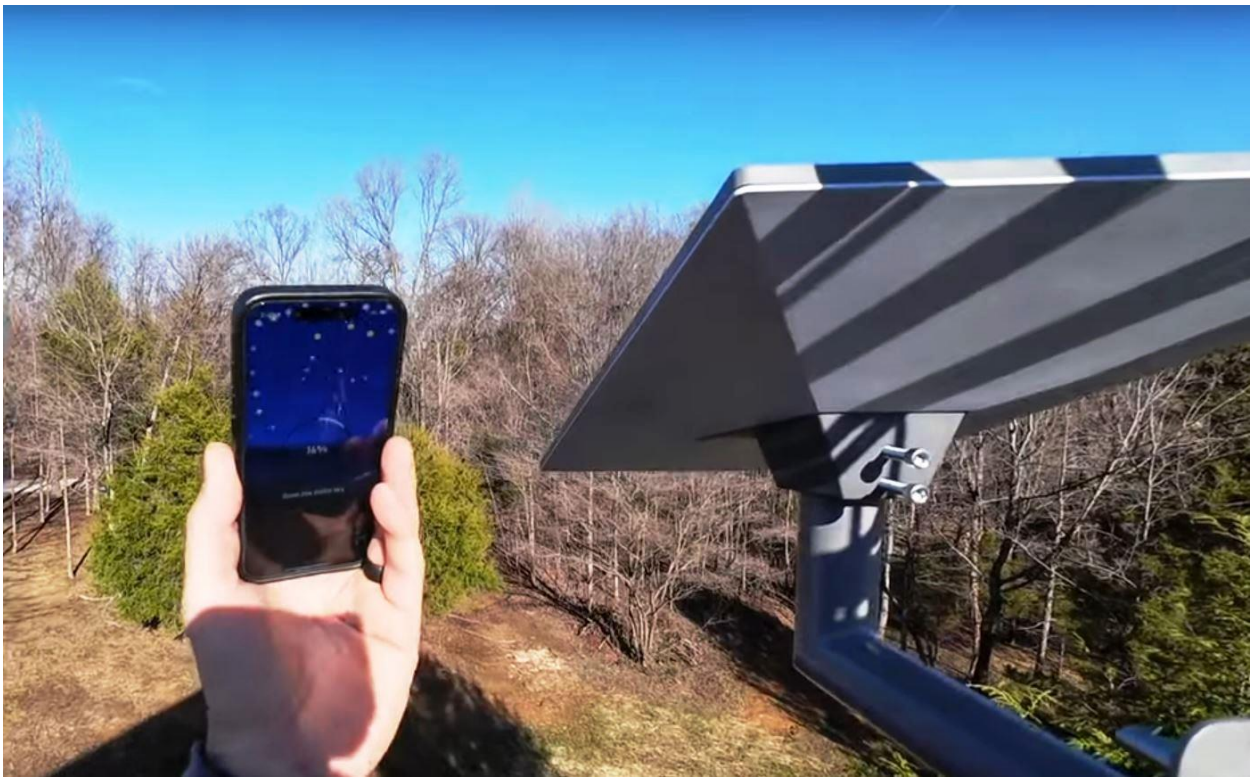
Users can most likely improve their speeds by bridging another (better) wired/wireless router to the Starlink router via the network port and marginally improve their wireless speeds, but dramatically improve their wired speeds via Ethernet cables.

So the real question becomes, how much in additional BEAD or other Federal subsidies will this system require right now, and into the future if the number of and quality of the satellites improves and especially if the bandwidth moves closer to the 1 Gbps current standard of a fiber land line connection? How tremendous would the cost be to eventually move to 10 Gbps?

For those of us who are not *city slickers* and live in northern wooded *fly over country*, it likely means 100 ft. towers. In the northern part of the northern states, from west coast to east coast, this would seem to be necessary. Hills, hollers, and valleys can also contribute to this requirement across the entire country.

Not sure that I want BEAD tax monies subsidizing this.

Is this you?



You have to get this "Dishy" above the trees

1) A Lattice tower costing between $10,000 and $20,000
2) Site Survey and Permits could cost anywhere from $500 to $3,000
3) Foundation Work: The foundation for a 100-foot tower range from $5,000 to $10,000, depending on the soil conditions and complexity of foundation design
4) Labor Costs: Labor to install the tower typically costs between $5,000 and $15,000

The total cost to erect a 100-foot antenna tower can range from $20,000 to $60,000 or more, depending on the specific circumstances.

Not sure that this is affordable to most anyone.

Sample Order Summary
Recurring Monthly Payment
Residential Starlink Subscription $120.00/mo.
One-Time Payment
Starlink Standard Kit $349.00 (includes router)
Congestion Charge $100.00
Shipping & Handling – Standard $20.00
Tax $18.45
Total $487.45

Note: this does not include any additional mounting hardware or networking equipment

Due to network congestion in your area, there is an additional one-time charge to purchase Starlink Residential services. Our intention is to not charge this fee to new customers as soon as network capacity improves. **(Isn't that just "special!" and I am in a very rural area)**

Note: this newer cheaper model dish/panel does not include the self-adjusting servo motors. So if you put it up high, (30 to 100 feet) and you likely will in rural non-flat areas, you will need to go up there to manually realign it if necessary, and it likely will be necessary at some point. You will also need to keep the 40 watt heater turned on, unless you want to climb up to remove the snow and ice.
So the real question becomes, how much in subsidies will this system require both now and into the future?

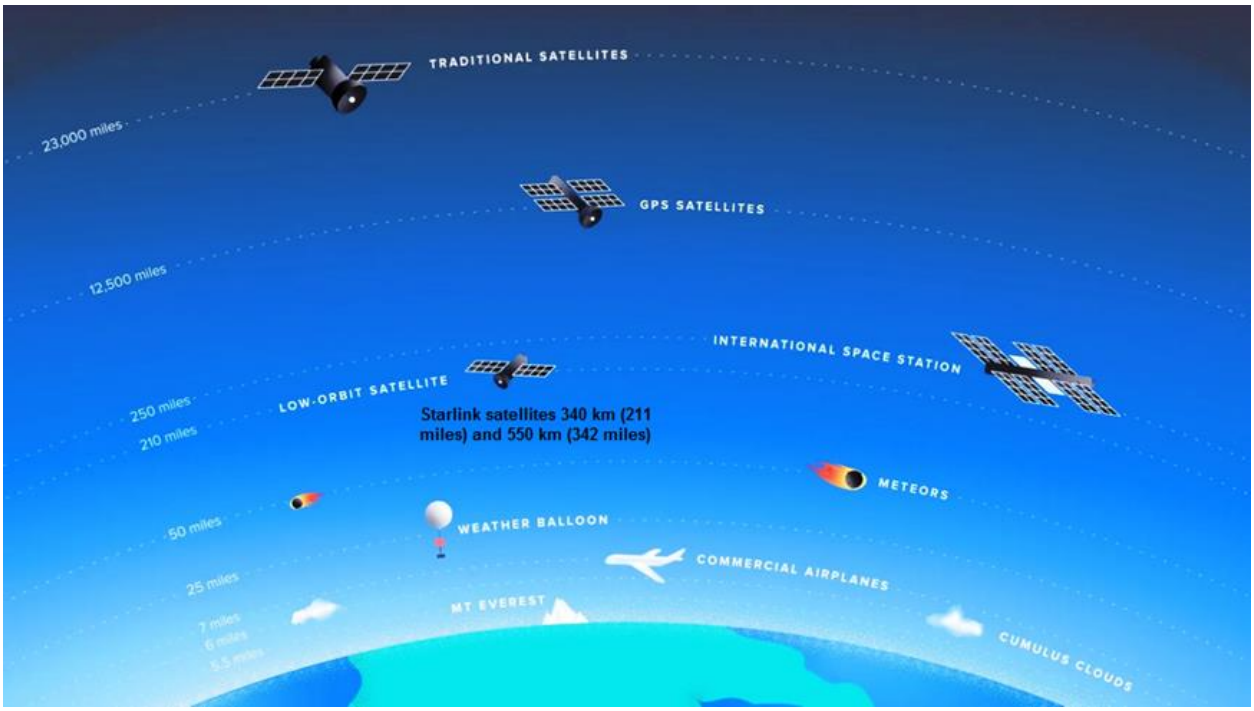
Some Important Research to Consider

Starlink does not strictly meet the target of 100/30 Mbit/s broadband connection when many Starlink users are active in the same geographical area, even though Starlink can provide *good enough* broadband. In particular, the target of 30 Mbit/s in uplink cannot be achieved with Starlink as the beam capacity, which must be shared among users, is only about 30 Mbps in the same geographical area, so the upload requirement cannot be met.

- Starlink's broadband service for many underserved addresses could represent a significant improvement compared to the service that underserved addresses have access to today
- Starlink is estimated to be able to provide a broadband connection with experienced data rates of 60-100 Mbit/s download and 5-10 Mbit/s upload1, corresponding to a satisfactory broadband service
- The tested user experience with broadband connection over Starlink is satisfactory with simultaneous use of streaming, browsing, video meetings, home office, etc.; only in demanding online gaming is the increased system latency in Starlink noticeable
- Like a HFC cable system, and unlike fiber or DSL, Starlink is a shared user system. The influx of subscribers is closed in certain areas to ensure that Starlink can provide a satisfactory service quality. In addition to fixed broadband solutions
- In xDSL, the connection from the distribution center to the individual address is one-to-one, i.e., dedicated per address, and one address will therefore not benefit from the fact that no data is used on another residual group address. The achieved data rate in downlink and uplink in xDSL is generally given by the distance from the distribution center to the address
- In Starlink, the quality of the satellite connection is typically the same for all users, but the connection is one-to-many (downlink), or many-to-one (uplink) within an antenna beam. The active users at the addresses must therefore share the beam capacity within the individual antenna beam
- The maximum data rate that a user can experience, the peak data rate, corresponds to the beam capacity of about 400 Mbit/s in downlink and about 30 Mbit/s in uplink. If the broadband target of 100 Mbit/s downlink and 30 Mbit/s uplink is understood in the

common sense, there will thus only be capacity for one user per beam in uplink and 4 users in downlink within an average geographical coverage area of 400 km2. In common sense, it is understood that the mentioned data rates are continuously achievable, e.g., as a result of a speed test. Due to the shared resource, this is therefore, strictly speaking, only possible with one user in the coverage area with a 100/30 Mbit/s broadband connection. More users will have to share the capacity

- **40 active users per antenna beam, all fully utilizing the connection, will on average be allocated 10 Mbit/s in downlink and 0.75 Mbit/s in uplink.** However, all users will experience peak data rates of 400 and about 30 Mbit/s in short intervals. In practice, the 40 users will not have continuous use of the data connection, and Starlink will therefore automatically distribute any available capacity in the beam according to the demand at the addresses within the beam's coverage area
- On latency during periods of the tests, system delays over Starlink were noted to be significantly greater than the average delay of 76 ms. As a reference, the analysis company Ookla measured a delay of 58-66 ms for Starlink in the USA from November 2022 to November 2023



What happened to the 2021 promise of 300 Mbps? Musk Reality Distortion Field (MRDF)

Speed will double to ~300Mb/s & latency will drop to ~20ms later this year
— Elon Musk February 22, 2021
https://www.teslarati.com/starlink-2x-speed-update-elon-musk/

Pricing

Starlink's service began during its 2022 beta phase, with prices around $99/month for limited service, but costs rose after the broader rollout, with the year 2023–2024 cost being $120. This does not include additional congestion charges, or hardware.

With a 2.5%, annual growth rate, under a moderate inflation scenario, the monthly price in 2030 would be approximately $138.96.

Note: to put this in perspective, 1000 Mbps symmetrical fiber optic Internet connections can be purchased in many locations around the country for $100 per month or less.

Postscript

Then there is this to consider

Elon Musk under Federal Investigation for Flouting Security Clearance Rules
https://www.msn.com/en-us/politics/government/musk-under-federal-investigation-for-flouting-security-clearance-rules/ar-AA1w6lWD
Elon Musk will not receive highest-level government security clearance – reports
https://www.pressreader.com/usa/the-guardian-usa/20241217/282385520113323

Literary Source References:

Report on broadband coverage for Starlink
rapport-om-bredbaandsdaekning-for-starlink_v11_23f3870011f54f52bc765acd32c3c479 english.pdf
What angle to the sky do you need for Starlink?
https://search.brave.com/search?q=what+angle+to+the+sky+do+you+need+for+starlink&source=desktop&summary=1&conversation=4c0bcc9192b95819e3b758
A Big Launch Year for Low Earth Orbit Satellites
https://broadbandbreakfast.com/a-big-launch-year-for-low-earth-orbit-satellites/
Maine, New Mexico Want Starlink Part of the Mix: Balancing Trade-Offs and Concerns
https://broadbandbreakfast.com/maine-new-mexico-want-starlink-part-of-the-mix-balancing-trade-offs-and-concerns/
Maine's Free Starlink Initiative Sparks Debate Over Rural Broadband Solutions
https://broadbandbreakfast.com/maines-free-starlink-initiative-sparks-debate-over-rural-broadband-solutions/
Maine to Hand Out Free Starlink Terminals to Unserved
https://broadbandbreakfast.com/maine-in-an-apparent-first-to-offer-starlink-to-9-000-unserved-locations/
Finally Installed STARLINK.....Is It Really BETTER??
https://www.youtube.com/watch?v=feZPPIl4wGs

This story was written by a human, not by Grammarly GO, ChatGPT, Jasper AI, GrowthBar, Frase, Copysmith, Hypotenuse, Copy AI, Writer, InferKit, Quillbot, Writesonic, Ryter, Gemini, or any other AI text generator.

SpaceX Requests Starlink Gen2 Modification, Previews Gigabit-Speeds (satellitetoday.com) 70

Posted by BeauHD on Thursday October 17, 2024 @03:00AM from the taste-of-the-future dept.

Longtime Slashdot reader schwit1 shares a report from Via Satellite: *SpaceX submitted a request to the FCC to modify the second generation, Gen2, of its Starlink satellite system with changes that SpaceX said will allow the constellation to deliver gigabit-speed broadband. SpaceX submitted the filing to the FCC on Oct. 11, and it was made public on Tuesday. The operator wants to make changes to the orbital configuration and operational parameters, and requests modifications for its Gen2 frequency authorization.*

These modifications "will enable the Gen2 system to deliver gigabit-speed, truly low-latency broadband and ubiquitous mobile connectivity to all Americans and the billions of people globally who still lack access to adequate broadband," Jameson Dempsey, SpaceX director of Satellite Policy said in the filing. For comparison, Starlink's current statement on service speeds is that users typically experience download speeds between 25 and 220 Mbps, and a majority of users experience speeds over 100 Mbps. In 2022, the FCC partially approved SpaceX to deploy a Gen2 Starlink constellation of up to 7,500 satellites for fixed satellite services (FSS) in the Ku- and Ka-bands, then later authorized Gen2 operations using additional frequencies in the E- and V-bands. SpaceX reported that since then, it has deployed more than 3,000 satellites in the Gen2 system and the full Starlink constellation serves more than four million people.

Starlink US residential customers are getting a limit on their high-speed internet

Users may find themselves on the 'Basic Access' service if their usage exceed 1TB of data in a month.

https://www.zdnet.com/home-and-office/networking/starlink-us-residential-customers-are-getting-a-limit-on-their-high-speed-internet/

In the US, Starlink's median download speed in the second quarter of **2022 hit just over 62 Mb**ps, according to the network intelligence firm Ookla. That's more than sufficient for one or two people to stream videos, download games or do whatever they want on the internet. However, a year prior, download speeds in the US were closer to **90 Mbps.**

https://www.zdnet.com/home-and-office/networking/starlink-satellite-internet-how-does-it-work-cost-features-speed/

The satellite Internet service provider is adding customers around the globe, but its growing popularity is affecting its performance.

https://www.zdnet.com/article/starlink-speeds-have-slowed-as-more-people-sign-up-report-shows/

The Hacking of Starlink Terminals Has Begun (wired.com) 16

Posted by BeauHD on Saturday August 13, 2022 @09:00AM from the like-any-emerging-technology dept.

AmiMoJo shares a report from Wired: *Since 2018, ELON Musk's Starlink has launched more than 3,000 small satellites into orbit. This satellite network beams internet connections to hard-to-reach locations on Earth and has been a vital source of connectivity during Russia's war in*

Ukraine. Thousands more satellites are planned for launch as the industry booms. Now, like any emerging technology, those satellite components are being hacked. Today, Lennert Wouters, a security researcher at the Belgian university KU Leuven, will reveal one of the first security breakdowns of Starlink's user terminals, the satellite dishes (dubbed Dishy McFlatface) that are positioned on people's homes and buildings. At the Black Hat security conference in Las Vegas, Wouters will detail how a series of hardware vulnerabilities allow attackers to access the Starlink system and run custom code on the devices.
To access the satellite dish's software, Wouters physically stripped down a dish he purchased and created a custom hacking tool that can be attached to the Starlink dish. The hacking tool, a custom circuit board known as a modchip, uses off-the-shelf parts that cost around $25. Once attached to the Starlink dish, the homemade printed circuit board (PCB) is able to launch a fault injection attack -- temporarily shorting the system -- to help bypass Starlink's security protections. This 'glitch' allows Wouters to get into previously locked parts of the Starlink system. The researcher notified Starlink of the flaws last year and the company paid Wouters through its bug bounty scheme for identifying the vulnerabilities. Wouters says that while SpaceX has issued an update to make the attack harder (he changed the modchip in response), the underlying issue can't be fixed unless the company creates a new version of the main chip. All existing user terminals are vulnerable, Wouters says. Wouters is making his hacking tool open source on GitHub. Following his presentation, Starlink says it plans to release a "public update" to address the issue but additional details were not shared.

FCC Cancels $886 Million In Funding For SpaceX's Starlink (pcmag.com) 146
Posted by BeauHD on Thursday August 11, 2022 @03:00AM from the application-denied dept.
The FCC is canceling $886 million in funding for Starlink to expand access in rural areas, citing the satellite internet system's cost and doubts over whether it can supply fast enough speeds. PC Magazine reports: *The agency today announced it had rejected "long-form applications" from both SpaceX and an ISP called LTD Broadband to secure funding from the FCC's Rural Digital Opportunity Fund. "The Commission determined that these applications failed to demonstrate that the providers could deliver the promised service," the FCC said in a statement. FCC Chairwoman Jessica Rosenworcel added: "We cannot afford to subsidize ventures that are not delivering the promised speeds or are not likely to meet program requirements."*
In December 2020, the FCC awarded $886 million to SpaceX to help its Starlink service supply high-speed broadband to 642,925 locations in 35 states. However, it came with a requirement that SpaceX provide a long-form application about how Starlink would meet its obligations before the federal funding could be fully secured. The FCC's goal with the Rural Digital Opportunity Fund is to supply gigabit internet speeds to over 85% of the selected rural locations and at least 100Mbps download speeds for all 99.7% of the locations in the coming years.
"Starlink's technology has real promise," Rosenworcel said. "But the question before us was whether to publicly subsidize its still developing technology for consumer broadband -- which requires that users purchase a $600 dish -- with nearly $900 million in universal service funds until 2032."

This is the twelfth in a series of articles on Broadband Internet

An Informed Citizens View of the Current Broadband Fiber Kerfuffle (Part Three)

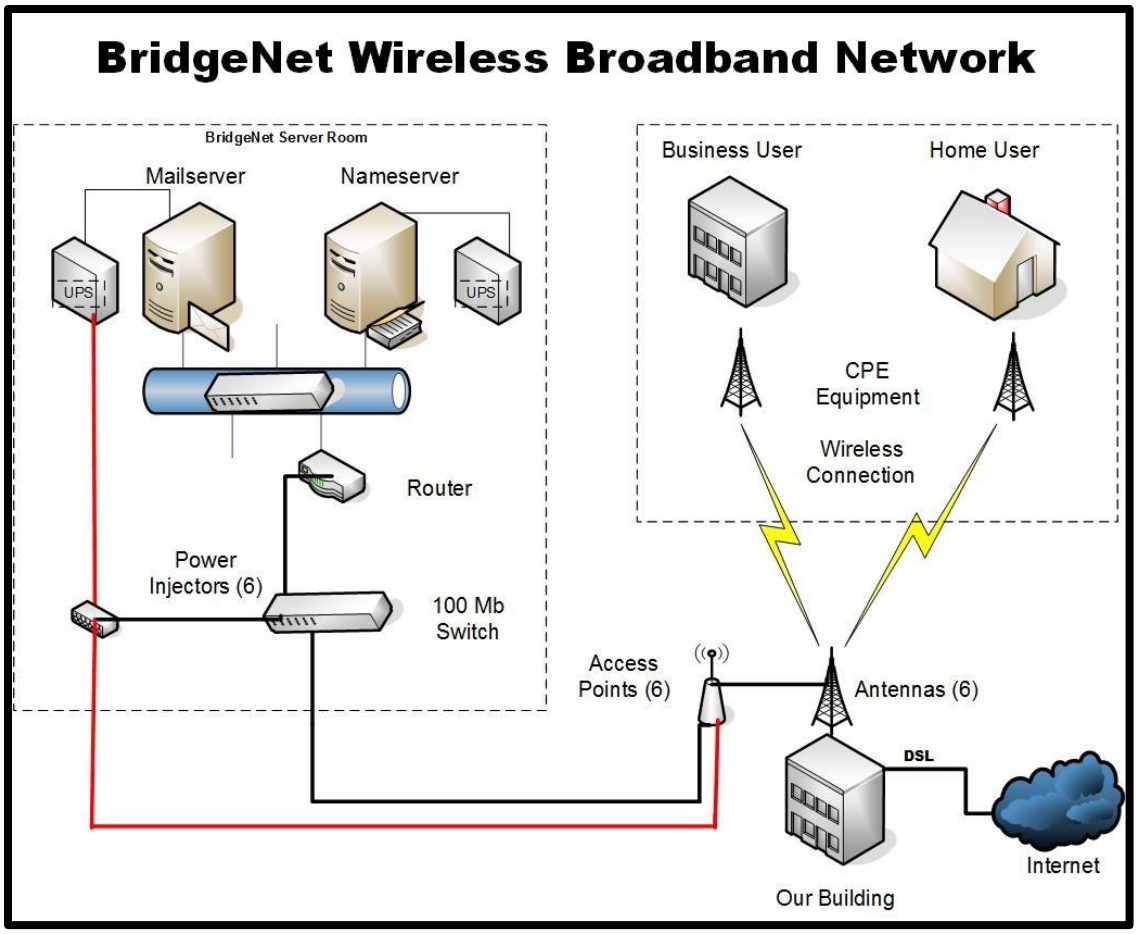
(You think WISP's are an answer, but why would someone even consider tax funding this?)

Dishes, antenna's and transmitter/receivers, Oh, My!

All Fixed Wireless broadband technologies suffer from the same issues.

Note: Look, I am a former WISP and recent user of a Wireless Internet Service Provider or WISP in both urban and rural settings. However, their time has passed and their usefulness as a bridge in the transition from dialup through ISDN, DSL, T1's T3's and HFC cable, to future proof terrestrial fiber networks has come and gone. These people are the heroes of a day gone by, like the BBS hosts. For a brief point in time, I was proud to be one of them, a simple neighborhood example of one anyway. (See americas-broadband-heroes-fixed-wireless-2011.pdf)

BridgeNet Neighborhood WISP



Urban BridgeNet WISP

Antennas

and Servers

Some Pros of Fixed Broadband Wireless

1. Quality signal—Fixed wireless delivers a higher-quality signal than other types of wireless Internet because its transmissions are focused directly toward the receiver on your home or business and not scattered in multiple directions. It also uses a much higher frequency than many other wireless technologies, which allows more information to be transmitted, resulting in higher bandwidth. Many cellphones top out at 25 Mbps.

2. Simple infrastructure—Because sending signals wirelessly is more cost-effective than building the infrastructure to send a signal via a wired connection, ISPs can expand their service areas quickly without a lot of up-front costs. This business advantage is particularly helpful for smaller ISPs or ISPs just entering the market. Fixed wireless generally works well in mountainous areas where transmitters can be placed at high elevations to reach a wider range.

3. Local ownership—Many fixed wireless providers were started by local entrepreneurs. Most fixed wireless providers are small, local businesses with ties to the surrounding community.

Some Cons of fixed wireless

1. Signal obstruction—Fixed wireless Internet transmitters require a clear line of sight from one transmitter to another in order to function. Ensuring that lines of sight remain clear can be problematic because an ISP can't always control what happens between one transmitter and another. A tree could grow taller, another company could construct a tall building, a pole could get knocked over by adverse weather which could potentially disrupt a fixed wireless transmission.

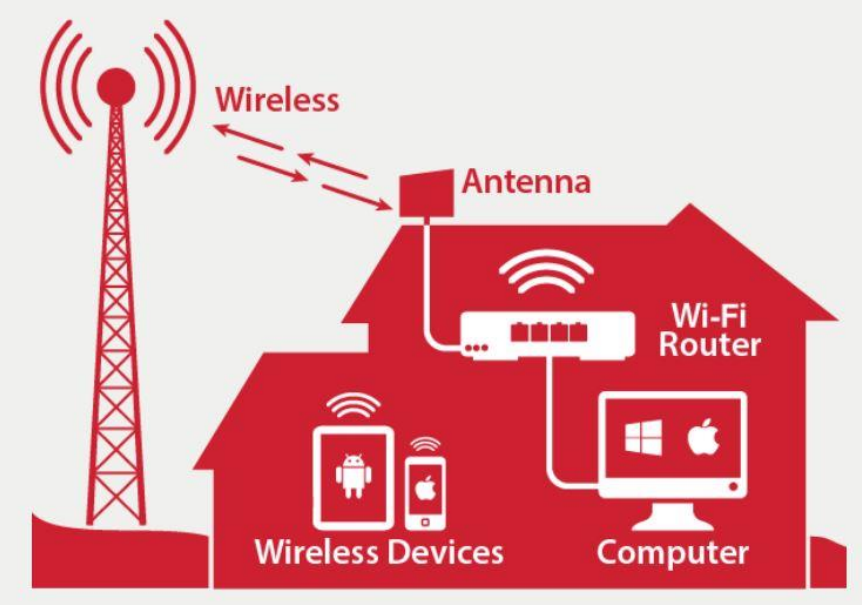
2. While low frequency transmissions like radio and television can easily pass through small obstructions and even walls, the short wavelength used by fixed wireless can be more easily deflected by foliage and similarly sized objects.

3. Limited availability—Although fixed wireless networks offer some of the fastest, most reliable connections available in rural areas, there just aren't many fixed wireless networks in operation. Only around a third of the rural population has access to fixed wireless Internet.

Note: Actual speeds may vary widely depending on network conditions between your location and the destination location, which includes Internet backhaul traffic beyond the local networks control. Typical speeds assume wired connections with the users' devices. Wi-Fi speeds are affected by factors such as home network congestion, signal strength, and interference. Network performance also varies by factors such as time of day congestion, signal strength, interference, and weather.

How fixed wireless Internet works

Fixed wireless networks—also known as fixed wireless access (FWA), broadband wireless access (BWA), wireless Internet service providers (WISPs), and several other terms—work by sending a wireless signal directly from a remote transmitter to a receiver on your home. While cell towers transmit in all directions within a given radius to serve mobile customers, fixed wireless transmitters send signals directly to other fixed wireless transmitters.



Fixed wireless signals

Fixed wireless providers use a variety of technologies in their networks. The main distinction between fixed wireless connections and cellular technologies is that fixed wireless connections cannot be moved and require line of sight (or near line of sight) to the transmitter.

Another difference between fixed wireless and cellular connections is the equipment involved. Cellular equipment usually consists of a single device within the home, which may have a separate antenna that is placed in a window. Fixed wireless connections usually have an external antenna or dish mounted on the outside of the house to maximize signal strength. This is then connected to the customer premises equipment (CPE) where you plug in your router (or the CPE might have a router built in). In multifamily buildings like apartments, the entire building might be connected to the network with a single antenna and CPE, which is then connected to routers in each individual household.

With the development of 4G LTE home Internet and 5G home Internet, which both sacrifice mobility to provide a stronger signal, the distinction between fixed wireless and cellular providers is becoming even more blurred.

Fixed wireless infrastructure

Fixed wireless providers work similarly to most landline networks, but they use wireless transmitters instead of running cables underground. Not only does this configuration save on the up-front costs of building a network, but it also allows for a strong and fast Internet connection within that network.

These wireless transmitters connect in two different ways, point-to-point (PtP) and point-to-multiple-point (PtMP). The antennas that connect to all the residential customers in a given area use PtMP, with one tower providing a signal to multiple homes. These antennas then use direct PtP connections to send the signal toward the backbone of the provider's network (a high-bandwidth fiber connection), which then connects to the backbone of the Internet.

Fixed wireless antennas can also be much smaller (and cheaper to build) than cell towers. However, to get the most out of their range, they need to be mounted someplace high. Tall buildings and mountains make excellent spots to mount antennas. But, in flatter areas, providers might have to build towers just to keep the signals from being blocked by the curvature of the earth.

The expansion of fixed wireless

Fixed wireless technology has been around for a long time, but it's seen more growth as more frequencies of the spectrum are opened up for commercial use. For example, another chunk of the spectrum was opened in 2015, allowing fixed wireless providers to use frequencies that were previously reserved for government uses like radar.

Also, since fixed wireless networks can make use of unlicensed spectrum bands (where equipment has to be able to function while causing minimal interference to other users), new fixed wireless networks can be deployed rapidly while dealing with fewer regulations.

One of the biggest challenges for fixed wireless networks is their asymmetric speeds. Like many other connection types, fixed wireless networks often deliver much higher download speeds than upload speeds. This is ideal for many high-bandwidth activities, like streaming movies and downloading files; however, as online habits shift toward things like video chat, telehealth, and livestreaming, upload speed is becoming more important.

This shift is reflected in government programs like the USDA's ReConnect Program, which requires providers to offer symmetrical speeds of at least 100Mbps in order to qualify for funding. This could make it difficult for fixed wireless providers, many of whom are small local companies, to keep up with the expense of new technologies and equipment.

Bridging the Digital Divide

Although fixed wireless isn't as fast as fiber or as exciting as cutting-edge satellite technology, it might be one of the fastest and easiest ways to address the digital divide. It might however expose a high cost in maintenance and upgrades versus future proof fiber networks.

Fixed wireless vs. other wireless connections

There are a many varieties of wireless Internet, and fixed wireless is just one specific kind. Fixed wireless Internet is different from satellite Internet, Wi-Fi, 4G, and 5G.

Fixed wireless vs. satellite Internet

Satellite Internet works using transmitters orbiting Earth. This technology allows for high availability, but also results in high latency. Because fixed wireless is based on the Earth's surface, it may have lower latencies than satellite, but may also provide higher speeds and lower prices, as well.

Fixed wireless vs. Wi-Fi

Wi-Fi is the technology used to connect small wireless Local Area Networks (LANs). For example, your home Wi-Fi network or the Wi-Fi at your favorite coffee shop both manage the Internet connections for all the devices on their respective networks.

Wi-Fi is a set of wireless network protocols based on the on the IEEE 802.11 standards. Its radio signals work well even in crowded areas where the airwaves are filled with other Wi-Fi signals, though it can be blocked by walls, pillars, and other solid obstructions.

Most people use Wi-Fi for their home networks, but they still need a way to connect their home network to the Internet. This connection could be a wired connection like cable or fiber, or you could connect to the Internet wirelessly over a connection like fixed wireless.

Fixed wireless vs. Mobile Broadband

Mobile broadband is a catch-all term for Internet connections used on mobile devices like your phone, tablet, or a wireless hotspot. Fixed wireless, as you might expect, is designed with the expectation that both the transmitter and receiver are in fixed locations, so even if you could take the antenna off your house and stick it to a car, it likely wouldn't work.

Fixed and mobile wireless Internet plans tend to have different use cases. Although many people rely on their phones as their only connection to the Internet, it's more common for people to have both. There are, however, ways to use these same cellular networks to make connections designed for home Internet, which is where 4G and 5G home Internet connections come in.

Fixed wireless vs. 4G home Internet and 5G home Internet

Fixed wireless is different from cellular technologies like 4G and 5G, though there is considerable overlap in the technologies they use. These wireless technologies are the same used in mobile phones that have Internet connectivity, but they can also be used for home Internet connections.

Although the technologies are similar to fixed wireless, the cellular towers used for 4G and 5G home Internet require more infrastructure, because they're also used to provide mobile coverage. Since these networks pull double duty, their top speeds are often a bit lower. Fixed wireless towers, on the other hand, are built with home Internet in mind, so they are often able to deliver higher speeds using just a few well-placed towers.

Analysis of Wisconsin WISP's

NETWURX
Up to 100 Mbps download x 20 Mbps upload
https://www.netwurx.net/residential.html
$149.95/mo.
Bertram Internet
Up to 100 Mbps download x 20 Mbps upload
https://www.gobertram.com/residential-services/
$249.95/mo
e-vergent LLC
Download: 15 Mbps Upload: 4 Mbps
https://www.e-vergent.com/residential-Internet/
$147.95/mo.
Bug Tussel Wireless, LLC
Up to 100 Mbps download x 20 Mbps upload
https://btussel.com/wireless-Internet-plans/
$149.95/mo.
Mercury Telecom
Typical Download Speeds 88–140 Mbps (Max 210 Mbps)
Typical Upload Speeds 8–20 Mbps
https://www.mercury.net/high-speed-Internet.php
$99.00/mo.
GigFire
500/250 Mbps
$110
https://www.gigfire.com/internet.html

Note: to put this in perspective, 1000 Mbps symmetrical fiber optic Internet connections can be purchased in many locations around the country for $100 per month or less.

Postscript

Then there is this to consider

Note: Terrestrial fiber optic cable and Digital Divide critic Brett Glass of LARIAT.NET, in Laramie, WY, sells Fixed Broadband Wireless to this city of 30k population, in our least populous state, for $150 and up with download from 65 to 1000 Mbps, depending upon location and equipment. Upload speeds are unknown. Laramie is situated on the flat Laramie Plains between the Laramie Mountains and the Medicine Bow Range.

Literary Source References:

America's Broadband Heroes: Fixed Wireless Broadband Providers
Delivering Broadband to Unserved and Underserved Americans
http://www.wirelesscowboys.com/wp-content/uploads/2011/10/americas-broadband-heroes-fixed-wireless-2011.pdf
About fixed wireless Internet
https://www.highspeedInternet.com/providers/fixed-wireless
ISPs keep giving false broadband coverage data to the FCC, groups say
Telcos accuse fixed wireless ISPs of claiming more locations than they serve.
https://arstechnica.com/tech-policy/2024/02/isps-keep-giving-false-broadband-coverage-data-to-the-fcc-groups-say/
Ceragon Networks offers wireless backhaul and fronthaul solutions for public and private networks
Robust wireless backhaul and fronthaul solutions, supporting speeds of 1-10 Gbps
https://www.ceragon.com/

For a **10 Gbps** wireless point-to-point link, you can generally expect to pay between $10,000 and $50,000 per system, with costs influenced by the equipment choice, installation needs, and additional services like support and licensing.
For a **1 Gbps** wireless point-to-point link, you can expect to pay significantly less (typically $2,500 to $15,000).

This story was written by humans, not by Grammarly GO, ChatGPT, Jasper AI, GrowthBar, Frase, Copysmith, Hypotenuse, Copy AI, Writer, InferKit, Quillbot, Writesonic, Ryter, Gemini, or any other AI text generator.

Note: This is the second of a four article series on Broadband Internet

An Informed Citizens View of the Current Broadband Availability Kerfuffle

(We all need to just get to work and resolve this problem)

Almost half of US residents don't use broadband Internet says study. Microsoft President Brad Smith put the number of nonusers at 162.8 million, almost half of the 329 million 2018 U.S. residents. Microsoft should know because they can measure ACTUAL bandwidth based on software updates delivered. Downloaded data size versus download time, equals download speeds.

- The Federal Communications Commission (FCC) estimates that 24.7 million Americans do not have access to broadband internet

This number seems wildly inaccurate due to random volunteer self-testing, flawed Ookla test results, the corporate corruption of the FCC Measuring Broadband America MBA Program, historically falsified FCC 477 bi-annual ISP voluntary report forms, (used to disadvantage competition), and the changing definitions of broadband in Mbps from 25/3, to 100/20. When what it should be in 2024 is 1000/1000.

- A 2020 Pew Research Center study revealed that 113 million people do not use broadband
- The National Telecommunications and Information Administration (NTIA) puts this number at, as of 2022, approximately one in five, or 24 million U.S. households that do not have a high-speed Internet service connection

Perhaps unknown political and bureaucratic reasoning's account for these mixed numbers.

What we do know is that those on the wrong side of this digital divide, and there are many, many, millions, are falling deeper into a second class citizen Caste, each and every year.

The Internet began as an Open system with few gatekeepers. We have since allowed the monopolization of telecommunications much as it was prior to the breakup of AT&T in 1982. Recent history shows that when AT&T was forced to share and compete over control of phone and DSL lines, this begat TDS, Frontier, and others offering the same services at lower prices. Competition works? Imagine that!

Here is some ancient history to help understand this.

FDR began a roll out of rural electrification across the whole nation from 1930 to 1950. People replaced candles and gas lanterns with electric lights and realized that this was great. Then they sought to replace steam and hit and miss engines on the farms. So…

- In the 40's came refrigerators, washing machines, radios, clothes dryers, telephones, water pumps, electric shaving razors, and food freezers. They paid more for the kilowatts used, but didn't need to upgrade to another tier of electrical service or technology, or settle for less.
- In the 50's came televisions, food mixers, electric heat, toasters, toaster ovens, coffee makers, electric fans, dishwashers, vacuum cleaners, electric clocks, electric knives, crock pots, electric power hand tools, electric table saws, bench grinders, pressure washers, mainframe and minicomputers, and microwaves. They paid more for the kilowatts used, but didn't need to upgrade to another tier of electrical service or technology, or settle for less.
- In the 60's to the 90's came personal computers, laser printers, UPS's, room air conditioners, water softeners, humidifiers and dehumidifiers, air compressors, electric motors, garage door openers, stereos, video cameras, hair dryers, cellphones They paid more for the kilowatts used, but didn't need to upgrade to another tier of electrical service or technology, or settle for less.
- In this century came, electric lawn mowers, and electric automobiles and other vehicles, massive computer datacenters, AI Chat bots. They paid more for the kilowatts used, but didn't need to upgrade to another tier of electrical service or technology, or settle for less.

In the 20 years between the early nineteen seventies and early nineties, the Internet was created and deployed. Packet-switched networks were created for the devices that needed digital connectivity, so then came dial-up, ISDN, DSL, fiber optic, HFC cable, terrestrial Fixed Broadband Wireless, Cellular Wireless, and then space based Satellite connection technologies. All of these technologies save fiber, had and still have limitations that prevent the expansion of the needed *future proof* bandwidth.

The point here being that we have little idea of what is coming at us with artificial intelligence, telehealth, remote working, and home based businesses, and digital home employment, or virtual education, virtual reality, and holography, in the future. This is just as they did not imagine the progress in the 1930's.

10 Gbps (10,000 Mbps) fiber connections are currently being installed and 50 Gbps and beyond of bandwidth is now technically possible.

Our governments and corporations have tried and failed to roll out unlimited bandwidth with fiber optic cables for the past 30 years. This has failed largely, not due to the $1.2 trillion of public monies, credits, and regulation relief given to the monopolies, but primarily caused by a lack of government regulation and competition.

Right now, the USA is at least ten years behind Europe and even further behind Asia on affordable and available Internet service. This fact puts this country at a competitive disadvantage in the world.

Broadband access is a non-partisan issue that need not divide us because when we all do well, we all do well.

By Michael F. Pitsch, December, 2024

His five novels are published on leanpub.com under the pseudonym Lefty Insider

"As we leave the Industrial Age and enter the Information Age, it's clear that despite all the technical advances and globalization, the formula for economic success has remained the same: economic prosperity relies on high-speed access to the critical network of information and commerce. That network is the Internet, and the type of access needed is broadband."
William Kennard, former Chairman of the Federal Communications Commission

Literary Source References:

Almost half of US residents don't use broadband internet: study
https://thehill.com/policy/technology/419898-1628-million-people-do-not-use-broadband-internet-in-us-study/

Following a proposal from Democrats that the federal government spend $80 billion funding the deployment of fast broadband — with upload/download speeds of 100Mbps — across underserved areas, AT&T is arguing that it's not worth the money because rural people should be happy with slower internet service than cities get. *"[T]here would be significant additional cost to deploy fiber to virtually every home and small business in the country, when at present there is no compelling evidence that those expenditures are justified over the service quality of a 50/10 or 100/20Mbps product,"* AT&T wrote in a blog post.
https://www.inverse.com/input/tech/att-doesnt-want-us-to-fund-fast-internet-in-rural-areas

FCC Measuring Broadband America
FCC/SamKnows ran these tests M-F /at 7-11PM for one month in September 2021. This was during the pandemic when the nationwide 2,750 tested residents' adults and students were at home using the Internet for work and school during the day. The Internet providers were aware of when the testing would be conducted, only in urban areas at the lowest speed tiers available.
https://data.fcc.gov/download/measuring-broadband-america/2022/Technical-Appendix-fixed-2022.pdf

Corporate monopoly breakups
https://en.wikipedia.org/wiki/BreakupoftheBellSystem

Countries with the fastest average fixed broadband internet speeds worldwide as of January 2024
https://www.statista.com/statistics/896772/countries-fastest-average-fixed-broadband-internet-speeds/

Ajit Pai touted false broadband data despite clear signs it wasn't accurate
https://arstechnica.com/tech-policy/2020/09/ajit-pai-touted-false-broadband-data-despite-clear-signs-it-wasnt-accurate

AT&T gave FCC false broadband-coverage data in parts of 20 states
https://arstechnica.com/tech-policy/2020/04/att-gave-fcc-false-broadband-coverage-data-in-parts-of-20-states/

Note: This is the third of a four article series on Broadband Internet

An Informed Citizens View of the Current Broadband Affordability Kerfuffle

(Why can't we make this service as affordable as electricity and water?)

But let me be very clear: Capitalism without competition isn't capitalism; it's exploitation. Without healthy competition, big players can change and charge whatever they want and treat you however they want."
Remarks by President Biden At Signing of An Executive Order Promoting Competition in the American Economy July 09, 2021.

New Analysis Shows Offline Households Are Willing to Pay $10-a-Month on Average for Home Internet Service, Though Three in Four Say Any Cost is Too Much

In the United States, Internet connection prices range from about $30 to $120+ per month, depending on the provider, type of network, speed tier, and temporary discounts. Some Internet providers offer discounted programs for low-income households. These are often designed to make Internet more accessible and typically provide speeds barely sufficient for essential tasks like browsing, email, and light streaming.

In other words, the lower cost programs require enrollment in a second class citizen Caste, previously written about.

So this is where we are at right now.

Effective June 1, 2024, the Federal Affordable Connectivity Program or ACP has ended and at least 23 million households enrolled in the ACP will no longer receive this discount.

The Affordable Connectivity Program (ACP) was a federal program that offered eligible households a discount of up to $30 per month toward Internet service. The ACP ran from December 2021 to June 2024 and as reported in February 8, 2024, over 23 million households relied on the program before the $14.2 billion in funding ran out.

The impacts of the end of the ACP:

1. Many low-income households would see their Internet bills increase by $30/month, which could push broadband costs out of reach. Households that rely on the ACP to make Internet service affordable might struggle to pay for full price Internet, especially if they were already paying for discounted programs like Xfinity Internet Essentials, Spectrum Internet Assist, or Cox Connect2Compete.
2. Many low-income households rely on the Internet for basic services, including education, healthcare, job searching, and government services. The end of the ACP disconnects or reduces Internet access for people who can't afford the full price, and the digital divide.
3. Students in low-income households relying on the Internet for schoolwork may struggle with remote learning or accessing educational resources. The digital divide has already created a disparity in access to online learning tools. Students in low-income families will face challenges with online classes, homework, and research.
4. Without the program, broadband adoption rates in low-income areas could decline. Many families may choose to forgo Internet access altogether, missing out on opportunities for education, remote work, and personal growth.
5. Low-income individuals may find it more difficult to access online job applications, participate in remote work, or expand their skills through online training or resources. Many job opportunities and services are only online, so the loss of affordable Internet can hinder economic mobility for those who need it most.
6. The burden will shift to local governments and community organizations, which might have to increase their efforts to provide free Wi-Fi or Internet subsidies. These services are limited in scope and as easily accessible.
7. Internet access will be made more unaffordable for a large portion of the population, leading to greater digital exclusion. People who cannot afford broadband would be unable to participate fully in digital society, including online voting, digital healthcare, or participating in the modern workforce, leading to greater social and economic inequalities, and unrest and loss of hope.
8. Many low-income households rely on the Internet to access telehealth services or online medical appointments. Without affordable Internet, these families might be unable to access healthcare remotely, especially in rural or underserved areas. The telemedicine boom during the pandemic has shown the importance of digital access for healthcare delivery, and its loss could negatively impact public health outcomes.

9. Low-cost Internet programs provided by ISPs, could become even more critical, however these programs often offer speeds that are insufficient for online education, or working from home.
   On the upside:

- Proponents of the Affordable Connectivity Program argue that the subsidy essentially pays for itself. A recent economics working paper estimated that for every dollar spent on the ACP, the nation's gross domestic product increases by $3.89.
- A study from the Chamber of Progress, calculated that ACP subscribers would lose $10 billion in work opportunities, $1.4 billion in telehealth savings, and $627 million in student benefits, if the program ends. The Benton Institute study found that the lost economic benefits from online shopping alone amounted to $1.5 billion.

The end of the US government's Affordable Connectivity Program (ACP) is now resulting in disconnection of Internet service for Americans with low incomes. Charter Communications reported a net loss of 154,000 Internet subscribers that it said was mostly driven by customers canceling after losing the federal discount. About 100,000 of those subscribers were reportedly getting the discount, which in some cases made Internet service free to the consumer.

The end of the ACP will likely result in higher costs for low-income households, reduced access to essential services, and greater digital exclusion. It is crucial that policymakers consider the long-term benefits of the ACP and work to ensure that affordable Internet access remains available to those who need it most.

I think that we can all do better.

By Michael F. Pitsch, December, 2024

His five novels are published on leanpub.com under the pseudonym Lefty Insider

"A popular Government without popular information or the means of acquiring it, is but a Prologue to a Farce or a Tragedy or perhaps both. Knowledge will forever govern ignorance, and a people who mean to be their own Governors, must arm themselves with the power knowledge gives".—JAMES MADISON Letter to W.T. Barry, Aug. 4, 1822, in G.P. Hunt, ed., IX The Writings of James Madison 103 (1910).

Literary Source References:

2022 Analysis Shows Offline Households Are Willing to Pay $10-a-Month on Average for Home Internet Service, Though Three in Four Say Any Cost is Too Much

Our analysis shows affordability as a driving factor around why some households continue to remain offline, confirming that cost of service is an essential part of increasing Internet adoption.

https://www.ntia.gov/blog/2022/new-analysis-shows-offline-households-are-willing-pay-10-month-average-home-Internet

Affordable Connectivity Program Has Ended

https://www.fcc.gov/sites/default/files/ACP-FAQs-Post-ACP-Ending.pdf

ChatGPT 4.0 mini

https://chatgpt.com/ "What are the impacts of the end of the ACP?"

The Harsh Reality for the 23 Million Americans Hit by the End of ACP Support

https://www.cnet.com/home/internet/the-harsh-reality-for-the-23-million-americans-hit-by-the-end-of-acp-support/

The contribution of US broadband infrastructure subsidy and investment programs to GDP using Input-Output modeling

https://arxiv.org/ftp/arxiv/papers/2311/2311.02431.pdf

Analysis: Low-income Americans will take a $20 billion hit when the Affordable Connectivity Program expires

https://progresschamber.org/wp-content/uploads/2024/04/Analysis_-Economic-Impact-of-ACP-Expiration-050124.pdf

Low-income homes drop Internet service after Congress kills discount program

https://arstechnica.com/tech-policy/2024/07/low-income-homes-drop-internet-service-after-congress-kills-discount-program/

Biden praises ISPs for price cuts even as they "sabotage" his FCC nominee

https://arstechnica.com/tech-policy/2022/05/biden-praises-isps-for-price-cuts-even-as-they-sabotage-his-fcc-nominee/

Leaving Money on the Table: The ACP's Expiration Means Billions in Lost Savings

https://www.benton.org/publications/acp-expiration-means-billions-lost-savings

This is the fourth of a series of articles from this author regarding Broadband Internet

An Informed Citizens Report from the Consumer Internet Trenches

(We can write our own ending to this story, because it doesn't need to be this hard to protect ourselves)

We've all heard the story. Computers were supposed to be the great equalizer, the tools that would free us from the tyranny of centralized power and create a new world of democracy and participation. They would be our passports to a better future—one where the Internet was a wide-open space, free from corporate control and surveillance.

The irony, of course, is that computers were in fact once the great liberators. They were tools for democratizing knowledge, empowering creators to create content, and tearing down the old barriers of access to information, and engage in political movements. The rise of the Internet only seemed to make this promise even clearer—this vast, open space where anyone with an Internet connection could share their voice.

For a brief moment, it felt like we were on the verge of something revolutionary.

But somewhere along the line, something happened. The revolution was hijacked, and the architects of this digital world—the ones who have built the infrastructure of surveillance and control that underpins our lives—have found ways to turn the tools of freedom into mechanisms of oppression.

So let's get real here. The computer revolution didn't bring freedom. It brought centralization. It brought surveillance. It brought a new kind of corporate oligarchy that controls not just the products we use, but the very systems that govern our lives. Computers are now being used to reinforce a new era of exploitation.

It's time we face the facts: we've been sold a lie.

Computers have become the lifeblood of our world—ubiquitous, essential, and increasingly misunderstood. From the silicon heart of our smartphones to the sprawling server farms that power the cloud, computers dictate not only the way we communicate, work, and live, but also how we think. But here's the catch: as we surrender more and more of our agency to these machines, we also face a stark reality: the more we rely on computers, the more power we give to the corporations and governments who control them.

The Promise of Computers: Democracy and Access

Some of us remember the early days of the internet. It was a decentralized space where anyone with a modem and a dream could set up shop, publish their thoughts, and share their creations. It was a time when the digital commons seemed boundless, a place where individual empowerment was just a click away. But those days are gone. In their place is a walled garden, meticulously cultivated by tech giants who have turned the open web into their private domain.

When personal computers first started making their way into homes across the globe, we were promised that they would empower the average person. The digital revolution was supposed to democratize knowledge and tear down the walls between us and the powerful. We imagined a world where media monopolies would crumble, where governments couldn't control information, and where individuals could carve out their own niche in the digital space.

The shift has been subtle, almost invisible. With every click of the "Accept" button, with every app we download, we've handed over pieces of our sovereignty—data, behavior, preferences—to the companies that control the platforms. Facebook, Google, Apple, and Amazon: these are not just businesses, they are the gatekeepers of the digital universe. They control not just what we see, but how we see it. They decide which ideas get amplified, which ones get buried, which voices are heard, and which are silenced.

And we're not just talking about the data they collect from us. We're talking about how these companies control the very structure of our digital lives. How they manipulate algorithms to maximize engagement—and profit—by shaping our emotions, our preferences, our ideas. They know us better than we know ourselves, and they use that knowledge to sell us everything from consumer goods to political ideologies.

This isn't just about convenience. It's about control. Every like, every share, every search query—these aren't just personal actions. They are data points used to build a behavioral model of you. A model that companies can use to target you with ads, to influence your opinions, to predict your next move. We are not the customers of these *free* platforms; we are the product.

We're not just users of their platforms; we are the product. Our data—our lives—have been reduced to a commodity, packaged and sold to the highest bidder. What was once the promise of personal empowerment is now the engine of a surveillance economy that tracks our every move.

The Computer as a Tool of Control

The power of computers lies not just in their ability to process information, but in their ability to monitor and shape human behavior. Modern computing has enabled the development of algorithms that govern everything from the ads we see to the news we consume to the very jobs we are hired for. These algorithms don't just react to our behavior—they shape it. They push us toward certain choices, nudge us in particular directions, and condition us to think in ways that benefit their creators.

What is the cost of this "convenience"? It's a loss of autonomy. These systems don't just collect data about us—they use that data to predict, manipulate, and influence us. They create an invisible architecture of control that shapes our thoughts, desires, and even our identities. And it's all happening behind the scenes, hidden in the code that runs these systems.

But it's not just the corporations we need to worry about. Governments have eagerly embraced the same technologies of surveillance and control. The "War on Terror" gave rise to mass surveillance programs that trample on civil liberties in the name of security. The digital trail we leave every time we use our computers, our phones, our smart devices, is cataloged and analyzed, turned into a predictive model of our behavior. With facial recognition, location tracking, and ubiquitous monitoring, we have become the subjects of an unprecedented experiment in state control.

The Reality: The Silicon Tyranny

It is now clear that the revolution is over. We didn't win; nor lose, we were co-opted. The tech giants that were supposed to be the new rebels of the digital age have become the very embodiment of capitalist control. Apple, Google, Amazon, Facebook, Microsoft, IBM—they are the new monarchs, sitting atop an empire of data, extracting wealth from our everyday digital lives.

The Problem With Open Source: The Myth of Freedom

Now, don't get me wrong: there are alternatives to all this. Open-source software, the so-called "free software movement," is often held up as the solution to corporate-controlled computing. Yes, open-source software offers transparency to inspect and analyze this computer code, and the potential for users to reclaim control over their digital lives. The idea that anyone, anywhere, can inspect, modify, and distribute the code that runs on their machines is an act of profound liberation. It's a declaration that the systems we use to navigate the world should be transparent, open to scrutiny, and built by the people who use them. Open-source software isn't just about giving people the freedom to use code—it's about giving them the power to *control* it.

But it's important to recognize that even open-source alternatives are still operating within a broader system that is fundamentally flawed.

The problem isn't just that we're using proprietary software. It's that the entire infrastructure of digital capitalism is structured in a way that makes it difficult for real alternatives to thrive. The cloud, the apps, the ecosystems—they're all built on the same economic model that prioritizes profit over people. Even the open-source movement is not immune to this pressure. We're still dependent on platforms owned by billionaires who control the data that runs through them. And as long as that's the case, we're not really free.

The Hope of Open Computing

But it's not all doom and gloom. The beauty of computers, the reason they were revolutionary in the first place, is that they can be *remade*. The very same tools of control that are used to surveil and manipulate us can also be repurposed for liberation.

This isn't just an abstract idea—it's happening right now. There are open alternatives to nearly every corporate-controlled platform, from social networks like Mastodon to decentralized web protocols like IPFS. The tools that were once the exclusive domain of the elite are now being reclaimed by ordinary people, and with each line of code, we inch closer to a world where our computers are no longer agents of surveillance, but agents of change.

The Future: Computers for People, Not Profits

The future of computing is not about ceding control to the few who can afford to build billion-dollar platforms. It's about returning the power to the many. It's about building systems that work for us, not against us. It's about reclaiming the open, transparent, decentralized ethos that was the hallmark of the early internet. A future where computers are tools of empowerment, not instruments of oppression.

But this will not happen on its own. It will require a concerted effort to push back against the forces that seek to control us. It will require a commitment to the principles of privacy,

autonomy, and openness. And it will require all of us to be vigilant, to keep asking the hard questions, and to refuse to accept the status quo.

The computers of the future will be the ones we build. And if we're smart about it, they will be computers that serve us, not the other way around. The question is, will we have the courage to fight for that future?

"Computers make excellent and efficient servants, but I have no wish to serve under them." --Mr. Spock from Season 2, Episode 24 of the original Star Trek television series.

The Way Forward: Breaking the Chains of Digital Serfdom

So, where do we go from here? How do we reclaim the promise of the computer revolution? The answer isn't simple, but it starts with understanding that we're not just fighting a few bad actors. We're fighting a system—a system that has weaponized the very tools that were supposed to set us free.

We need to break the cycle of dependence on centralized platforms. We need to rebuild a decentralized Internet, one where users are in control, not the corporations. We need to prioritize privacy, data ownership, and transparency in our digital lives. That means supporting initiatives that challenge the corporate monopoly on the Internet, like Project Liberty and others, whether that's through decentralized social media platforms, or data co-ops. It's also crucial that we demand accountability from the governments that are complicit in this surveillance state. We need stronger privacy protections, laws that prevent the corporate capture of our personal data, and more robust oversight of the technologies that control our lives. We can't just rely on individual responsibility; we need collective action.

But above all, we need to be honest with ourselves. The revolution isn't coming unless we demand it. The tools are in our hands, but we need to use them—not just to consume, but to rebuild. Otherwise, the computer revolution will remain just another piece of the capitalist machine, and we will remain its unwitting pawns.

A Red Pill View Of The Current Realities

Over the past ten plus years so, surveillance capitalism and its corporate eminent domain data harvesting have increasingly become the bane of my own personal online existence. Warding off the personally impactful ill effects of this corporate malfeasance, has become a part time occupation for me and sucks much of the joy from my Internet experiences which date back to the halcyon days of the nineties and those Open Internet experiences.

In this century we have returned to the online service walled gardens and centralized controls of yesteryear with the new G-Mafia (Google, Microsoft, Amazon, Facebook, IBM, and Microsoft. This is wholly antithetic to the origins of the Internet and vision of the Internet elders.

God
@TheTweetOfGod
Mark Zuckerberg is one of the last people you should trust, and I mean that both literally and alphabetically.
1:42 PM · Mar 21, 2018
12,905 Retweets
50,321 Likes

We have now legalized and normalized the data harvesting vulture surveillance capitalism these new monopolies provide. But your data is you, it is who you are! You have the fundamental right to control how much of you that you reveal to others, just as you do in your offline world. You choose to share what financial and healthcare details are public.

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say." — Edward Snowden

If you store your data in the Cloud, it is just someone else's computer servers holding your social media accounts, photos, data backups, or storage. This corporation owns this data and can change their policies on how they treat it at any time. Much of your health care info in the EPIC database is stored on Amazon servers.

There are not any good reasons in my view that these parasitic and predatory overseers cannot be replaced by local community libraries, municipalities, and nonprofit agencies. These entities could exercise local control for local residents and consumers, using local protocols and policies that are tied into the larger networks.

As things stand right now:

- To be able to safely use Windows 10 or 11, I must make extensive use of multiple software utilities to kill corporate telemetry, data scraping, and defeat interruption annoyances, like advertising, and notifications, to protect my personal self from a once somewhat benevolent now turned malevolent Microsoft Corporation
- I am forced to use Firefox or Brave for web browsers as they minimize data collection unlike Google Chrome, Microsoft Edge, and others
- I am forced to use browser extensions like Privacy Badger, JShelter, Ghostery, DuckDuckGo Privacy Essentials, uBlock Origin, uMatrix, for ad blockers, content filtering, blocking iframes and scripts, and to block invisible trackers and also to send *questionably effective* Do Not Track signals to offending websites
- I need yet another browser extension to constantly verify the integrity and security of these extensions. A checker for the checkers, if you will
- I need to use Malwarebytes and/or SpyShelter to watch executable performance and protect from malware, spyware, automatically installed Potentially Unwanted Programs, or PUPS, and keyloggers
- I need to use a utility like T-Mac to spoof my computer MAC address to prevent local identification
- I need to apply custom settings to my web browser to:
    1. Block trackers and scripts that want to plant cookies, tracking content, cryptominers, and fingerprinters on my computer systems
    2. Force HTTPS-Only Mode which ensures an encrypted (non-readable) connection to the websites I visit
    3. Force Domain Name Service or DNS translators over HTTPS to send requests through an encrypted connection making it harder for others to see which website I access

- I need to use OpenDNS for phishing protection, content filtering, and DNS lookup in its own DNS servers, rather than my snooping ISP
- I need to use Brave Search, StartPage, Freespoke, or DuckDuckGo search to avoid being tracked and personal data being seized as a corporate asset and/or monetized by data brokers absent consent or permission
- I need to use a robots.txt file to prevent AI robot algorithms from scraping my website and training LLM's on my personally created and proprietary data
- I need to use a Virtual Private Network or VPN, if I want to keep my ISP from harvesting and monetize my connection history data, sometimes called digital exhaust, without my consent or permission, I need to use this VPN to disguise myself from them. This in turn reduces my bandwidth by about 50%, not from encryption overhead (10-20%) but from the rent-seeking ISP overselling their increasingly congested and insufficiently upgraded network

Now some or most of you, may think that all of this is a bit, or more than a bit, too much and that ignorance is in fact bliss. Or as John Lennon said, "*living is easy with eyes closed, misunderstanding all you see"*. But this situation really does affect you whether you realize it or not, and there is little hope of change in the status quo unless you understand it and it's ramifications to you personally that you internalize this. Realize as well the resulting loss of social cohesion and destruction of democracies here and around the larger world. Remember that when you are online these days, there is a corporate or government AI pointed directly at your brain through your eyes. It is manipulating your thoughts and actions whether you realize it or not!

"He's hell bent for destruction, he's afraid and confused, and his brain has been mismanaged with great skill." Bob Dylan License to Kill, Album: Infidels

It should go without saying that you should not use the Cloud (other people's server computers) like Google Cloud, Amazon (AWS), Apple, Microsoft Azure, TikTok, and especially Facebook (Meta) accounts. Online storage and backup sites like Dropbox, iCloud, Google Drive, MS OneDrive, Amazon Drive, are almost certainly scrapped by multiple AI's now or in the near future. There are no good reasons why your refrigerator, oven, washing machine, microwave, Roomba, or toothbrush, etc. should be Internet connected. There *are* many good reasons that they should not. If you have a Smart (sic) TV now, and you are streaming your television from the Internet, you are in fact being spied on. This secretly collected and pilfered data can and is used to show you advertisements and otherwise collected and monetized by many sources.

Microsoft has been recently exposed as using *Connected experiences in Microsoft 365*, to allow an AI to train on and analyze your Word and Excel documents. It is turned on by default and the data is retained indefinitely. The user must find the settings to *opt out* of this local data collection. It is unclear if this data is exfiltrated directly to Microsoft as of right now, and would likely require professional analysis of the many page Microsoft Terms of Service legalize novella to sort this out. These policies can and do change at any time without notice. Then there is the believability and trust issues, from a known malevolent corporation, with a history of security exploits, data exfiltration's and hacks.

To be clear however, Microsoft _does_ currently exfiltrate your data to train AI Large Language Models or LLM's (databases) from your interactions with Bing search, MSN Co-Pilot, and the advertisements that you click on. They and most all corporations have declared eminent domain on your digital data exhaust.

A new lawsuit filed by a current Apple employee accuses the company of spying on its workers via their personal iCloud accounts and non-work devices. From a report:

The suit, filed in California state court, alleges Apple employees are required to give up the right to personal privacy, and that the company says it can "engage in physical, video, and electronic surveillance of them" even when they are at home and after they stop working for Apple. Those requirements are part of a long list of Apple employment policies that the suit contends violate California law.

Bluesky's Open API Means Anyone Can Scrape Your Data for AI Training. It's All Public (techcrunch.com)

Bluesky, a social media company, says it will never train generative AI on its users' data. But despite that, "one million public Bluesky posts — complete with identifying user information — were crawled and then uploaded to AI company Hugging Face," reports Mashable (citing an article by 404 Media).

Conclusion

The government, under supposed constitutional protections, is not allowed to harvest this citizen data. With the pending corporate takeover of our government, will it be turned against us, "*whether we like it or not*?"

Corporations, currently unhindered by government regulations, have been so far been free to engage in what Harvard professor Shoshana Zuboff calls "*an economic system built on the secret extraction and manipulation of human data."* Your personal data now becomes corporate assets. Common law dating back to the 17th century says that "*possession is nine tenths of the law*," referring to the he ten or twelve points of the law at that time.

For those of you who only use your Smart (sic) phones to access the Internet, because you think it actually is a computer, you actually have no idea of what is going on with them. It is much, much, more difficult to exercise _any_ control over these devices at all. Many _smart_ people are dumping these devices and getting flip phones.

All of this is only going to get worse as AI and VR infect, control, manipulate, and perhaps eventually completely destroy the safe functionality and the dreams of the Open Internet conceived by the Internet Founders.

We can still make a different future. But it won't be handed to us. We'll have to fight for it, one byte at a time.

The time to act is long past overdue. This may be your last warning.

His five novels are published on leanpub.com under the pseudonym Lefty Insider.
He also publishes articles on medium.com under the same pseudonym.

"Today, as our snoopy tech firms hide in the skirts of our spies and law enforcement agencies, we have to get beyond the idea that this is surveillance capitalism. Truly, it's more akin to surveillance mercantilism: a fusion of state and commercial power." Technologist and Author Cory Doctorow

Literary Source References:

The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power
by Shoshana Zuboff, Nicol Zanzarella, et al.
Chokepoint Capitalism: How Big Tech and Big Content Captured Creative Labor Markets and How We'll Win Them Back
by Cory Doctorow and Rebecca Giblin
The Internet Con: How to Seize the Means of Computation
by Cory Doctorow
AI Is Only As Good As The Data That Trains It
https://www.forbes.com/councils/forbestechcouncil/2023/08/10/ai-is-only-as-good-as-the-data-that-trains-it/
AI in cloud computing: Benefits and concerns
https://www.techtarget.com/searchcloudcomputing/feature/AI-in-cloud-computing-Benefits-and-concerns
Watch Out: How to Stop Your Smart TV From Spying on You
https://www.pcmag.com/how-to/how-to-stop-smart-tvs-from-snooping-on-you
Is your vacuum cleaner spying on you? Because that would suck
https://blog.avast.com/is-my-roomba-spying-on-me
Explained: the Microsoft connected experiences controversy
https://www.malwarebytes.com/blog/news/2024/11/explained-the-microsoft-connected-experiences-controversy

This is the fifth article in a series on Broadband Internet

An Informed Citizens View of the Current Broadband CyberSecurity Kerfuffle (Part One)

(Why can't we make the Internet a safe place for our children, and grandchildren to live and work?)

OpSec is the term used by computer security professionals as shorthand for operational security. Keeping the bad guys from getting at your computer, or other Internet connected devices to be able to extract or exfiltrate your personal information. There are many, many, layers to this idea.

Reducing your attack surface, used to be easy as using an antivirus software, built-in operating system software firewall, and not using things like toolbars and widgets on your desktop.

It used to be bored teenagers and criminals doing this. Now it is nation states, corporations, and our own government. It is computer operating system companies like Microsoft and Apple. It is software makers.

If you are a Smart (sic) phone user, it is most all apps from App Stores. It is many, many, websites. It is almost everyone trying to monetize your information. Information is the new oil.

It is your Internet provider. Your email provider. Your website host.

It is phishing emails and text message spoofs. It is mysterious phone calls and voice mail messages.

First, a bit of history

The first version of the Internet was born as a science project of the Advanced Research Projects Agency of the United States Department of Defense, or ARPANET (developed primarily for military use), and funded mainly by US Government National Science Foundation (NSF) grant monies, which created the NSFNET. Senator Al Gore Jr. from Tennessee, was a visionary on this subject, and thus was instrumental in advocating for this funding. The ARPANET was fundamentally about linking static read-only scientific and academic materials together; to assist the DOD with advanced forward thinking research much of it being conducted at universities all around the country.

The World Wide Web also called the Surface Web or Clear Web (mostly encrypted, thus sometimes clear), is a part of the Internet. Some think that the Web is THE Internet, but it is not. Nor is Facebook, Google, Apple, Amazon, and Microsoft. They are just parts of the whole. It is now more than a billion websites that a typical search engine used now by more than three billion worldwide users. You access it with a web browser such as Microsoft Internet Explorer, Microsoft Edge, Google Chrome, Safari, Pale Moon, Brave, or better yet Mozilla Firefox.

> *"If security were all that mattered, computers would never be turned on, let alone hooked into a network with literally billions of potential intruders"*— Dan Farmer, computer security researcher, and programmer

Welcome to Surveillance Capitalism: The New Economy

Welcome to the age of *surveillance capitalism*. This is the dark side of the computer revolution, the part they didn't tell you about in the glossy pamphlets. Our every move is tracked, recorded, and analyzed by powerful algorithms that exist to control us. Every time we check our phones, browse the web, or use a smart device, we're feeding the system.

The U.S. and other powerful states have fully embraced surveillance technologies, using the same tools built by Big Tech to monitor our movements, behaviors, and even our thoughts. The "War on Terror" gave birth to mass surveillance programs that now extend far beyond their original mandate. What was once a tool for "national security" has become the foundation of a global system of digital control.

In the name of safety and convenience, we've accepted a new form of corporate-government surveillance that tracks everything we do. Our privacy is no longer a right—it's a commodity, bought and sold by the highest bidder.

Surveilled

(Abused and exploited)

Surveillance [ser-vey-luh ns, -veyl-yuh ns] noun

- a watch kept over a person, group, etc., especially over a suspect, prisoner, or the like
- continuous observation of a place, person, group, or ongoing activity to gather information
- attentive observation, as to oversee and direct someone or something

Surveillance is the monitoring of behavior, activities, or information for the purpose of influencing, managing or directing. This can include observation from a distance by means of electronic equipment, such as closed-circuit television, or interception of electronically transmitted information, such as Internet traffic. It can also include simple technical methods, such as human intelligence gathering and postal interception.

https://en.wikipedia.org/wiki/Surveillance

https://ssd.eff.org/en/module-categories/basics

The easiest way to STOP this from happening is to STOP using all personal, car, and home surveillance devices!

A neat guide on "Assessing Your Risks" from the Electronic Frontier Foundation:

https://ssd.eff.org/en/module/assessing-your-risks

Check your email account and phone numbers to see if they have been compromised.

Here are a few news stories for you to think about:

Google is disabling Xiaomi integrations on our devices' after a Nest Hub user picked up random pics from strangers' feeds

"Among the eight examples initially provided are a handful of disturbingly clear images showing a sleeping baby, a security camera's view of an enclosed porch, and a man seemingly asleep in a chair." A camera owner reported receiving still images from other random peoples' homes when he tried to stream content from his camera to a Google Nest Hub.

Android Police broke the story, and published some photos that are horrifying, privacy-wise, if legit. androidpolice.com

(Android Police is an American technology news and a blog dedicated to everything related to Android smartphones.)

Google responded:

"We're aware of the issue and are in contact with Xiaomi to work on a fix. In the meantime, we're disabling Xiaomi integrations on our devices."

Note: Xiaomi, is a Chinese designer and manufacturer of consumer electronics and related software, home appliances, automobiles and household hardware, with headquarters in Beijing, China.

2019- The year of voice assistant privacy dumpster fires

2019 was the "I Told You So" year for privacy advocates and voice assistants: the year in which every company that wanted you to trust them to put an always-on microphone in the most intimate places in your home. They were revealed to have allowed thousands of low-waged contractors to listen in on millions of clips, many of them accidentally recorded. Amazon, Google, Apple, Microsoft.

What's more and worse, is that these arms-length contractors who were getting your stolen audio were working under terrible conditions, in sweatshops where they were worked long hours, listening to potentially traumatizing audio Voice assistants have proven to be no more secure than any of Big Tech's other products.

The true believers in voice computing started to build voice assistants in full knowledge that these will not only be perceived as creepy, but that they will be creepy. These companies lie to their customers, and even to Congress, about whether this is going on.

A former data analyst who worked on Apple Siri transcriptions for several years says workers swapped horror stories during smoke breaks. A current analyst, asked to recount the most outrageous clip to come through, says it was something akin to a scene from Fifty Shades of Grey.

https://boingboing.net/2019/12/12/not-ok-google.html

Silicon Valley Is Listening to Your Most Intimate Moments

How the world's biggest companies got millions of people to let temporary workers analyze some very sensitive recordings.

She could not believe what she was hearing. She had been hired by a temporary agency for a vague job: transcribing audio files for Amazon.com Inc. For $12 an hour, she and her fellow contractors, or "data associates," listened to snippets of random conversations and jotted down every word. The clips included recordings of intimate moments inside people's homes.

https://www.bloomberg.com/news/features/2019-12-11/silicon-valley-got-millions-to-let-siri-and-alexa-listen-in

Amazon Workers Are Listening to What You Tell Alexa

A global team reviews audio clips in an effort to help the voice-activated assistant respond to commands. Tens of millions of people use smart speakers and their voice software to play games find music or trawl for trivia. Millions more are reluctant to invite the devices and their powerful microphones into their homes out of concern that someone might be listening.

Sometimes, someone is.

https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio

The Chilling Side Effects of Mass Surveillance

Nothing to Hide?

"He who does not move, does not notice his chains" – Rosa Luxemburg, German-Polish Marxist theorist, socialist philosopher, and revolutionary, editor (1871–1919)

The definition of "bad" may mean one thing to those who are "good," but the people in power have the last say in what "bad" means. Bad could be anything that impedes the government's ability to pursue its interests, or exercise its power.

Mark Zuckerberg, CEO and founder of Facebook, says privacy is no longer a ***social norm,*** *yet he has used his millions to create his own personal privacy by buying all the properties around his house.*

Surveillance impedes creativity and freedom of expression. People alter their behaviors to conform when they know that they can be watched at any time. Just like when you were a child under your parents watchful eyes.

A panopticon is a type of architectural design devised by an 18th Century English philosopher and social theorist. The concept is to allow a single person to observe all the members of a group or class. It was devised for prisons, but is also used in computer labs in schools, school buses. Since it is physically impossible for one person to observe all subjects at once, obedience is obtained by the threat that anyone can be watched at any time. The key to the design is that one person can watch any inmate, but the inmate cannot see the person, so you never know when you might be under surveillance.

A society in which people can be monitored at all times is a society that breeds conformity, obedience and submission, and why every tyrant likes this.

It is important however in a free and democratic society, to have the whistleblowers, journalists, and other activists who can to provide a balance to those who are in power. Mass surveillance severely curtails this ability.

The measure of how free a society is, is not how it treats its compliant citizens, but how it treats its whistleblowers, journalists, activists, dissidents, criminals, as well as its poor and disenfranchised.

The US and its partners, unknown to the entire world until the Snowden file leaks, has converted the Internet, once heralded as an unprecedented tool of liberation and democratization, into an unprecedented tool of mass, indiscriminate predatory corporate capitalist surveillance. The totalitarian state that George Orwell foretold of in his book 1984, and it has stripped us of our personal privacy and freedoms.

There are many issues that face our future generations, but the erosion of our personal privacy, freedoms, and liberties is a clear and present danger. 250 years ago, people fought those who opposed the ideals of life, liberty, and pursuit of happiness. Those principles are the foundation that allowed the rise of the United States of America. Now, that very foundation is being eroded using the half-cocked excuse of keeping us safe.

https://www.aljazeera.com/opinions/2013/6/25/the-chilling-effects-of-surveillance/

https://www.techdirt.com/2016/05/02/chilling-effect-mass-surveillance-quantified/

"When Congress passed the Communications Assistance for Law Enforcement Act (CALEA) in 1994, they were assured by then-FBI Director Louis Freeh that the mandated wiretap backdoors posed no security risks."

https://leisureguy.ca/2024/10/16/fbi-arrogance/

So take a guess at who found it and is wiretapping us all of us now?

US Officials Urge Americans to Use Encrypted Apps Amid Unprecedented Cyberattack (nbcnews.com) 56

Posted by EditorDavid on Wednesday December 04, 2024 @03:30AM from the encryption-now-good dept.

An anonymous reader shared this report from NBC News: *Amid an unprecedented cyberattack on telecommunications companies such as AT&T and Verizon, U.S. officials have recommended that Americans use encrypted messaging apps to ensure their communications stay hidden from foreign hackers...*

In the call Tuesday, two officials — a senior FBI official who asked not to be named and Jeff Greene, executive assistant director for cybersecurity at the Cybersecurity and Infrastructure Security Agency — both recommended using encrypted messaging apps to Americans who want to minimize the chances of China's intercepting their communications. "Our suggestion, what we have told folks internally, is not new here: Encryption is your friend, whether it's on text messaging or if you have the capacity to use encrypted voice communication. Even if the adversary is able to intercept the data, if it is encrypted, it will make it impossible," Greene said. The FBI official said, "People looking to further protect their mobile device communications would benefit from considering using a cellphone that automatically receives timely operating system updates, responsibly managed encryption and phishing resistant" multi-factor authentication for email, social media and collaboration tool accounts...

The FBI and other federal law enforcement agencies have a complicated relationship with encryption technology, historically advocating against full end-to-end encryption that does not allow law enforcement access to digital material even with warrants. But the FBI has also supported forms of encryption that do allow some law enforcement access in certain circumstances.
Officials said the breach seems to include some live calls of specific targets and call records (showing numbers called and when). "The hackers focused on records around the Washington, D.C., area, and the FBI does not plan to alert people whose phone metadata was accessed."
"The scope of the telecom compromise is so significant, Greene said, that it was "impossible" for the agencies to predict a time frame on when we'll have full eviction."

Dozens of Countries Hit in Chinese Telecom Hacking Campaign, Top US Official Says (msn.com) 31
Posted by EditorDavid on Sunday December 08, 2024 @03:34AM from the do-you-hear-what-I-hear dept.
China-linked spies may still be lurking in U.S. telecommunications networks — but the breach could be much, much wider. In fact, a "couple dozen" countries were hit by the attack, the Wall Street Journal reported this week, citing a top U.S. national security adviser. "Chinese government hackers have compromised telecommunications infrastructure across the globe as part of a massive espionage campaign..." *Speaking during a press briefing Wednesday, Anne Neuberger, President Biden's deputy national security adviser for cyber and emerging technology, said the so-called Salt Typhoon campaign is ongoing and that at least eight telecommunications firms in the U.S. had been breached... The Journal previously identified Verizon, AT&T, T-Mobile and Lumen Technologies among the victims... [M]etadata grabs appeared to be "regional" in focus, and were likely a means to identify phone lines of valuable senior government officials, which the hackers then targeted to steal encrypted text messages and listen in on some phone calls, the official said... President-elect Donald Trump, Vice President-elect JD Vance, senior congressional staffers and an array of U.S. security officials were among scores of individuals to have their calls and texts directly targeted, an intelligence-collection coup that likely ensnared their private communications with thousands of Americans, the Journal has reported.*
The senior administration official said the global tally of countries victimized was currently believed to be in the "low, couple dozen" but didn't give a precise figure. The global campaign of hacking activity dates back at least a year or two, the official said.
"Neuberger, on the press briefing, said that it wasn't believed that classified communications were accessed in the breaches."

"If you think technology can solve your security problems, then you don't understand the problems, and you don't understand the technology." — Bruce Schneier, security expert

America's Phone Networks Could Soon Face Financial - and Criminal - Penalties for Insecure Networks (msn.com) 23

Posted by EditorDavid on Sunday December 08, 2024 @11:34AM from the tin-cans-and-a-string dept.
The head of America's FCC "has drafted plans to regulate the cybersecurity of telecommunications companies," reports the Washington Post, and the plans could include financial penalties phone network operators with insufficient security — "the first time the agency has asserted such powers under federal wiretapping law." *Rosenworcel said the FCC's authority in this matter comes from Section 105 of the Communications Assistance for Law Enforcement Act [passed in 1994] — a single sentence that stipulates, without elaboration, that telecommunications carriers should ensure systems security "in accordance with regulations prescribed by the Commission." As one of the measures, she is seeking to require network providers to submit an annual certification to the FCC that they are implementing a cybersecurity risk management plan. In addition to imposing fines, the FCC could coordinate with other agencies to pursue criminal penalties against carriers deemed too careless on cybersecurity...*

Biden administration officials said voluntary efforts to protect against aggressive Chinese hacking activity have fallen short. "We've had for the last decade voluntary public-private partnership efforts," Neuberger told The Post in a recent interview. "But we continue to see successful breaches, and in many cases, as with ransomware attacks, we continue to see pretty basic cybersecurity practices not being followed." With China's hackers becoming more brazen, pre-positioning themselves in U.S. critical networks, "we need to lock our digital doors," Neuberger said...

Cyber requirements can make a difference, she said. After the Colonial Pipeline ransomware attack in 2021 shut down one of the nation's largest energy pipelines for several days, creating a national security scare, the Transportation Security Administration issued several security directives, and today, all of the country's several dozen critical pipeline companies are in compliance, she said. Similar directives were subsequently issued for rail and aviation sectors, and the compliance rates in those industries are now at 68 and 57 percent respectively, she said.

More information as well as additional protection tools will be outlined in future additional parts of this article.

This author's five novels are published on leanpub.com under the pseudonym Lefty Insider.
He also publishes articles on medium.com under the same pseudonym.

"We're responsible for the creation of the PC industry. The whole idea of compatible machines and lots of software — that's something we brought to computing. And so it's a responsibility for us to ***make sure that things like "security" don't get in the way of that dream.*** *You know, its individual empowerment, information at your fingertips — we need to drive that forward."*

"One-on-One with Bill Gates" Chairman of Microsoft. Interview with Peter Jennings, abcnews.go.com. February 16, 2005.

Literary Source References:

Schneier on Security
https://www.schneier.com/books/
A User's Guide To The Dark Web (and Clear Web)
(The 42nd and Final Encyclopedia Cyberspacia)
By Lefty Insider (arister0s n0stis)
https://leanpub.com/encyclopediacyberspacia
Big Brother in the Wires: Wiretapping in the Digital Age
https://www.aclu.org/documents/big-brother-wires-wiretapping-digital-age

This is the sixth article in a series on Broadband Internet

An Informed Citizens View of the Current Broadband CyberSecurity Kerfuffle (Part Two)

(Why can't we make the Internet a safe place for our children, and grandchildren to live and work?)

OpSec is the term used by computer security professionals as shorthand for operational security. Keeping the bad guys from getting at your computer, or other Internet connected devices to be able to extract or exfiltrate your personal information. There are many, many, layers to this idea.

Offense versus defense

One of the reasons that the US government, and thus US corporations, are so susceptible to hacking is the overall attitudes that a good offense is more important than a good defense.

The government hoards and buys zero day exploits to use against targets. By not eliminating these exploits, and using them instead, everyone becomes susceptible to them. Now we may have criminal AI's tasked with looking for them.

A zero-day (also known as a 0-day) is a vulnerability in software or hardware that is typically unknown to the vendor and for which no patch or other fix is available. The vendor has zero days to prepare a patch as the vulnerability has already been described or exploited.

https://en.wikipedia.org/wiki/Zero-day_vulnerability

The Obama administration ordered NSA to disclose the security flaws it discovers in computer systems in most cases, but to hold those flaws in secret when they can be used to serve "a clear national security or law enforcement need." WannaCry is an excellent example of what can happen when an institution hoards zero-days.

Cybersecurity experts have raised significant concerns about the practice of governments hoarding zero-day exploits, particularly when they are used for intelligence or national security purposes. Here's a breakdown of key perspectives:

Security Risks to Citizens and Infrastructure: Experts argue that hoarding zero-day vulnerabilities — flaws in software that are unknown to the vendor and thus unpatched — puts both citizens and critical infrastructure at risk. While governments may use these exploits for cyber espionage, surveillance, or offensive cyber operations, these flaws can remain unpatched, leaving systems vulnerable to attacks by other actors, including criminal hackers. This practice is especially concerning in sectors like healthcare, energy, and finance.

Moral and Ethical Concerns: Many experts believe that withholding information about zero-days contradicts the ethical responsibilities of those who discover them. Vulnerabilities, when not disclosed and patched, create opportunities for exploitation. The question arises whether it is right for governments to prioritize using zero-days for covert operations over ensuring the broader public's safety.

Balance between Offensive and Defensive Cyber Capabilities: Some cybersecurity professionals acknowledge that intelligence agencies and governments might need to hoard some exploits for legitimate defense and offense, particularly in the context of cybersecurity warfare. However, they warn that there needs to be a careful balance. Excessive reliance on offensive capabilities can undermine overall cybersecurity, and the uncoordinated use of zero-days could weaken the security posture of various organizations and even governments themselves.

Impact on the Software Ecosystem: Another concern is the effect hoarding exploits has on the software ecosystem. Vendors and developers are generally at the mercy of external disclosures (or lack thereof) to patch vulnerabilities. When governments withhold information, it delays patching, leaving users and organizations vulnerable to cyberattacks for longer periods. Some experts advocate for stronger rules about responsible disclosure to ensure that vulnerabilities are patched swiftly.

Calls for Transparency and Regulation: A growing number of cybersecurity professionals call for more transparency in the government's handling of zero-days. There is a push for frameworks like the "Vulnerability Equities Process" (VEP), which the U.S. government uses to evaluate whether to disclose a vulnerability or retain it for intelligence purposes. While the VEP is a step forward, experts argue that it needs to be more transparent and include more oversight to avoid prioritizing intelligence operations over public safety.

In short, while the practice of hoarding zero-day exploits is seen as a legitimate tool for governments' offensive cyber operations, there is significant concern among cybersecurity professionals that it creates unnecessary risks. There is a call for a more balanced approach that prioritizes public safety while maintaining national security needs.

Then there are the American corporations working against you.

Data Brokers

China's Great Firewall, the UK's Snooper's Charter, the US' mass surveillance and bulk data collection -- compliments of the National Security Agency (NSA) and Edward Snowden's whistleblowing -- Russia's insidious election meddling, and countless censorship and communication blackout schemes across the Middle East are all contributing to a global surveillance state in which privacy is a luxury of the few and not a right of the many.

As surveillance becomes a common factor of our daily lives, privacy is in danger of no longer being considered an intrinsic right -- and it seems we, too, are adopting our own personal forms of online digital stalking and spying.

Digital bread crumbs, cookies (not necessarily a bad thing) to remember you but have now evolved to third party cookies that track you wherever you go, location, IP address, device, screen size. This is a bad thing.

Data brokers like Epsilon sell this info to anyone who will buy it.

Why is this a problem?

Your personal info not protected by HIPPA. The 4th Amendment does not protect you here. Any restrictions can be bypassed by the government simply buying information from these brokers.

The United States has **no** data privacy regulations like the European Charter of Fundamental Rights and The European Union's General Data Protection Regulation (GDPR).

Ransomware

Ransomware is malware (malicious software) planted unknowingly in a computer or mobile device that disables its operation or access to its data, until the owner pays a ransom fee to regain control or access.

https://www.dictionary.com/browse/ransomware?s=t

Ransomware attacks are typically carried out using a Trojan that is disguised as a legitimate file, that the user is tricked (see Phishing) into downloading or opening when it arrives as an email attachment.

https://en.wikipedia.org/wiki/Ransomware

Organizations that are cleaning up after a ransomware outbreak typically will change passwords for all user accounts that have access to any email systems, servers, and desktop workstations within their network. Ransomware victims fail to grasp that the crooks behind these attacks can and frequently do siphon every single password stored on each infected endpoint. The result of this oversight may offer attackers a way back into the affected organization, access to financial and healthcare accounts, or — worse yet — key tools for attacking **the victim's various business partners and clients**.

The point here is you could be infected by or have your login credentials stolen by one of your vendors or customers that have been attacked. For example:

- -Identity and password management platforms Auth0 and LastPass
- -Multiple personal and business banking portals;
- -Microsoft Office365 accounts
- -Direct deposit and Medicaid billing portals

- -Cloud-based health insurance management portals
- -Numerous online payment-processing services
- -Cloud-based payroll management services
- -Prescription management services
- -Commercial phone, Internet and power services
- -Medical supply services
- -State and local government competitive bidding portals
- -Online content distribution networks
- -Shipping and postage accounts
- -Amazon, Facebook, LinkedIn, Microsoft, Twitter accounts

How can you defend against ransomware?

1. Update your software. Use anti-virus software and keep it up-to-date. Set your operating system, (this is somewhat dubious advice as Microsoft seems to create as many flaws as they fix) web browser, and security software to update automatically on your computer. On mobile devices, you may have to do it manually. If your software is out-of-date, it is easier for criminals to sneak bad stuff onto your device.
2. Think twice before clicking on links or downloading attachments and apps. According to one panelist, **91% of ransomware is downloaded through phishing emails**. You also can get ransomware from visiting a compromised site or through malicious online ads.
3. Back up your important files. From tax forms to family photos, make it part of your routine to back up files on your computers and mobile devices often. When you are done, log out of the cloud and unplug external hard drives so hackers cannot encrypt and lock your back-ups, too.

If you are a victim of ransomware

1. Disconnect infected devices from your network to keep ransomware from spreading.
2. Restore your computer. If you have backed up your files, and removed any malware, you may be able to restore your computer. Follow the instructions from your operating system to re-boot your computer, if possible.
3. Contact law enforcement. Report ransomware attacks to the Internet Crime Complaint Center or an FBI field office. Include any contact information (like the criminals' email address) or payment information (like a Bitcoin wallet number). This may help with investigations.

Should you pay the ransom?

Law enforcement does not recommend paying the ransom, although it is up to you to determine whether the risks and costs of paying are worth the possibility of getting your files back. If you pay the ransom, there is no guarantee you will get your files back. In fact, agreeing to pay signals to criminals that you have not backed up your files. Knowing this, they may increase the ransom price — and may delete or deny access to your files anyway. Even if you do get your files back, they may be corrupted.

https://www.consumer.ftc.gov/blog/2016/11/how-defend-against-ransomware

How to Recognize and Avoid Phishing Scams

Scammers use email or text messages to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts. Scammers launch thousands of phishing attacks like these every day — and they are often successful. The FBI's Internet Crime Complaint Center reported that people lost $30 million to phishing schemes in one year. But there are several things you can do to protect yourself.

https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Pay some attention to what you are doing online and you will be fine.

Malware

Malware (a portmanteau for malicious software) is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive users access to information or which unknowingly interferes with the user's computer security and privacy.

Many types of malware exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wiper, and scareware. The defense strategies against malware differs according to the type of malware, but most can be thwarted by installing antivirus software, firewalls, applying regular patches to reduce zero-day attacks, securing networks from intrusion, having regular backups and isolating infected systems.

https://en.wikipedia.org/wiki/Malware

Botnets

Botnets are networks of hijacked computer devices used to carry out various scams and cyberattacks. The term "botnet" is formed from the word's "robot" and "network." Assembly of a botnet is usually the infiltration stage of a multi-layer scheme. The bots serve as a tool to automate mass attacks, such as data theft, server crashing, and malware distribution.

https://www.kaspersky.com/resource-center/threats/botnet-attacks

https://en.wikipedia.org/wiki/Botnet

Think your Data is Safe in the Cloud?

Your identity is ***not Safe in the Cloud!*** How can Microsoft Azure, MS OneDrive, and Google AWS protect your systems and data, if they cannot protect their own?

Cloud Identity is promoted as a great thing these days. You can sign up to lots of services using your social identity from Facebook, Google, or from Microsoft. You do not have to invent new passwords (or reuse passwords used elsewhere), and you get easy Single Sign On. This is sold as having more advantages than drawbacks for users, with little awareness of some of the dangers.

Think two factor authentication will protect you in the cloud. Think again. Even if an organization requires multi-factor authentication at sign-in, recall that a malware login process can take place on Microsoft's own Web site. In fact, many of these malicious actors host their evil doing directly on Microsoft Azure sites. That means having two-factor enabled for an account would do nothing to prevent a malicious app that has already been approved by the user from accessing their emails or files. They use malicious a Microsoft Office 365 App to gain access to a victim's account without requiring them to give up their credentials to the attackers.

"In the digital era, privacy must be a priority. Is it just me, or is secret blanket surveillance obscenely outrageous?" —Al Gore, former senator, vice president and avid supporter of the NSF

This author's five novels are published on leanpub.com under the pseudonym Lefty Insider. He also publishes articles on medium.com under the same pseudonym.

Literary Source References:

Schneier on Security
https://www.schneier.com/books/

A User's Guide to the Dark Web (and Clear Web)
(The 42nd and Final Encyclopedia Cyberspacia)
By Lefty Insider (arister0s n0stis)
https://leanpub.com/encyclopediacyberspacia

Governments pay millions for 0days: more harm than good?
https://cybernews.com/editorial/governments-pay-millions-for-0days-more-harm-than-good/

U.S. government is 'biggest buyer' of zero-day vulnerabilities, report claims
https://www.csoonline.com/article/546112/u-s-government-is-biggest-buyer-of-zero-day-vulnerabilities-report-claims.html

Additional Cloud Security Sources:

https://krebsonsecurity.com/2020/01/tricky-phish-angles-for-persistence-not-passwords/ - more-50056

https://securityintheenterprise.blogspot.com/2019/11/microsoft-azuread-and-office365-not.html

https://info.phishlabs.com/blog/office-365-phishing-uses-malicious-app-persist-password-reset

https://duo.com/blog/gmail-oauth-phishing-goes-viral

https://krebsonsecurity.com/2020/01/phishing-for-apples-bobbing-for-links/

This is the seventh in a series of articles on Broadband Internet

An Informed Citizens View of the Current Broadband CyberSecurity Kerfuffle (Part Three)

(Why can't we make the Internet a safe place for our children, and grandchildren to live and work?)

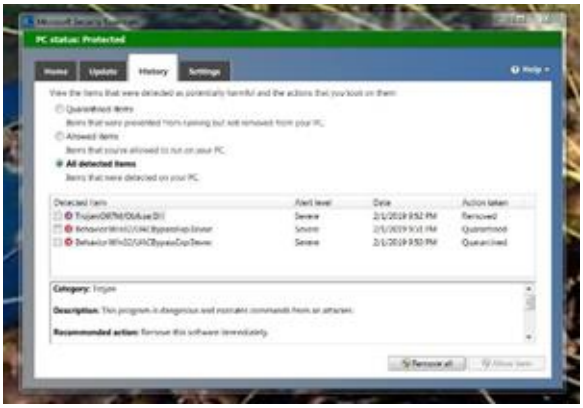
OpSec is the term used by computer security professionals as shorthand for operational security. Keeping the bad guys from getting at your computer, or other Internet connected devices to be able to extract or exfiltrate your personal information. There are many, many, layers to this idea.

The following identifies some tools that can be used to assist you with your own personal cybersecurity protections.

Microsoft Security Essentials (Windows Defender)

Microsoft Security Essentials (MSE) is an antivirus software (AV) product that provides protection against different types of malicious software, such as computer viruses, spyware, rootkits, and Trojan horses. Prior to version 4.5, MSE ran on Windows XP, Windows Vista, and Windows 7, but not on Windows 8 and later versions, which have built-in AV components known as Windows Defender. MSE 4.5 and later versions do not run on Windows XP. The license agreement allows home users and small businesses to install and use the product free-of-charge.

Microsoft Security Essentials automatically checks and downloads the latest virus definitions from Microsoft Update which is updated three times a day.



Note: MS has greatly improved this technology, originally labeled by users as their DCS technology. (Doesn't Catch Shit)

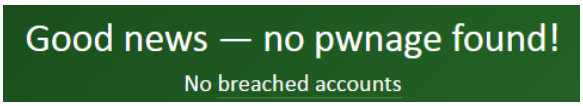
Malwarebytes Anti-Malware

Malwarebytes Anti-Malware is an anti-malware software for Microsoft Windows, MacOS and Android OS that finds and removes malware.

https://www.malwarebytes.com

Have I Been Pwned? (Hacker slang for owned)

https://haveibeenpwned.com/



ShieldsUp

https://www.grc.com/shieldsup

ShieldsUp is an online port scanning service created by Steve Gibson of Gibson Research Corporation and hosted at grc.com. The purpose of this utility is to alert the users of any ports that have been opened through their firewalls or through their NAT routers. The utility can scan the most common file sharing ports, as well as all service ports, and user defined ports, in sets of 64.

Encrypting Outlook email on the Clear Web (Internet)

https://blog.encyro.com/how-to-encrypt-email-in-outlook/#method-3-outlook-encryption-add-ins

https://support.microsoft.com/en-us/office/encrypt-email-messages-373339cb-bf1a-4509-b296-802a39d801dc

Are you leaking IP and ID info?

Protecting of your identify is desirable on the Internet. As OpSec has multiple layers, these are some.

IP Leaks

Testing for IP leaks is easy. All you need to do is connect your VPN and visit an IP leak website. Popular choices include:

browserleaks.com
ipleak.net
ipleak.org
ipleak.com
dnsleaktest.com

Compare the results from these sites with the VPN connected and with it disconnected. If any of the IP addresses that appear are the same before and after connecting to the VPN, then you have a leak.

Note: Make sure your VPN is not active.

1. Visit **WhatIsMyIPAddress.com** and note down the IP address. You can also choose to open Ethernet adapter to find the IP address.
2. Activate your VPN software, and select a remote server of your choice. Make sure it's working.
3. Post a few minutes, revisit WhatIsMyIPAddress.com and note down the IP address.
4. These two IP's should be different.

Domain Name Service, DNS, Leaks

Go to dnsleaktest.com or dnsleak.com (or any other DNS leak test tool you trust).

WebRTC IP Leak

All the major web browsers (such as Google Chrome, Mozilla Firefox, Safari, Opera, and Yandex) have a feature called web real-time communication, or WebRTC. This tool enables video calls, file sharing, live chats, voice calls, etc. But websites can trick the browsers' WebRTC feature into bypassing the website visitors' VPN IP address and revealing their real IP address through the use of JavaScript.

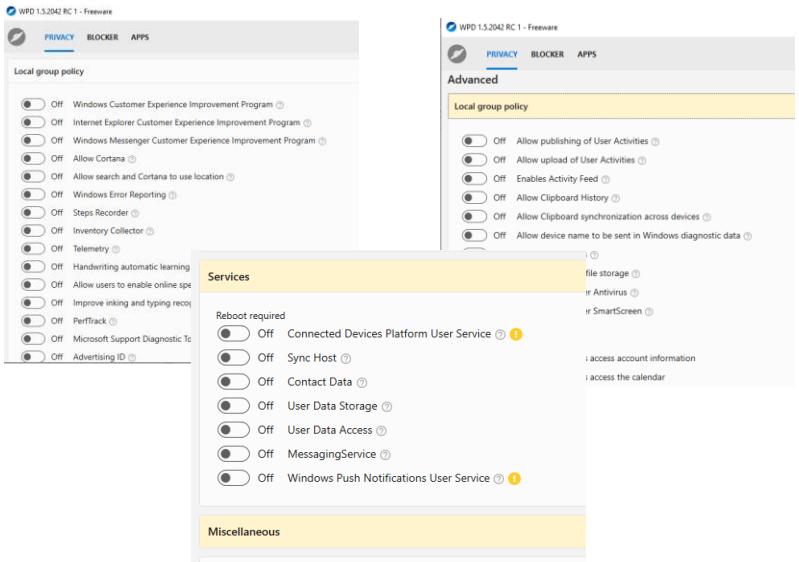
Even though there are tools available to conduct a WebRTC leak test, just do so with caution. You can't rely on them 100% because you don't know which websites are using special JavaScript to find out your real IP via WebRTC.

https://addons.mozilla.org/en-US/firefox/addon/happy-bonobo-disable-webrtc/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

Windows Privacy Dashboard

A small but powerful portable tool that works through the Windows API. WPD is the most convenient way to configure various privacy settings in Windows.

https://wpd.app/



How to prepare Windows 7 Ultimate 64 bit for the Internet

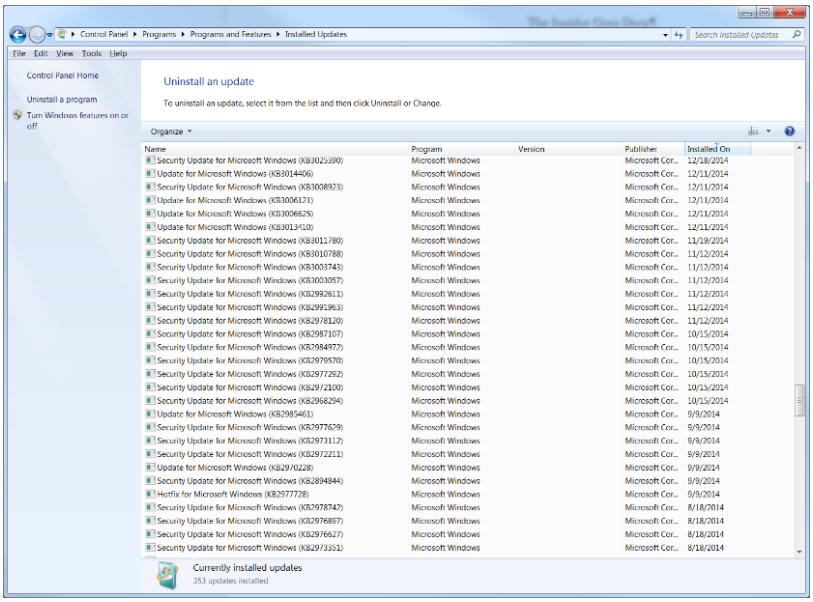
Do not even think about using Windows 8, 10, or 11 as they are originally configured. They are far too chatty across the Internet and incorporate telemetry, notifications, keylogging, and most recently advertising. All of these can make you easy to identify. There are however some tips that follow.

With Windows 7, starting in 2014, all updates especially those marked as *Security* are suspect. See my book, The Cozening, for more detail on this. These updates are mostly for preparation for Windows 10 and incorporate the MS belief that they are allowed to control your computer since you are using their software, whether you bought it or not.

Start with a clean install of Windows 7 64-bit Service Pack 1, build 7601.

Do a custom install and eliminate anything unnecessary to install. Running this inside of a Virtual Machine (Virtual Box) or not is up to you, but not necessary in my experience. It really depends or how comprehensive your backup strategy and OpSec are.

Your updates should stop at SP1, with a few exceptions. Some .net framework updates may need to be installed for certain programs to run.


Control Panel ▸ Programs ▸ Programs and Features ▸ Installed Updates
File Edit View Tools Help
Control Panel Home
Uninstall a program
Turn Windows features on or off
Uninstall an update
To uninstall an update, select it from the list and then click Uninstall or Change.
Organize
Name
Program
Version
Publisher
Installed On
Currently installed updates

You should eliminate (uninstall) or spay and neuter all Adobe products if you can as they are chatty as well. Since I need pdf's for these books, I control it with my firewall and the other hardening software mentioned elsewhere here.

Do not install any software that is not absolutely necessary for your purposes.

Aside from software updates and telemetry, where does Windows leak IP and ID info?

Assume a tuned and hardened Windows 7 bare bones system, updates off since SP1, updates off in registry and disabled. No Win10/11 so No Cortana, No OneDrive.

- TMAC for changing (spoofing) your MAC address
- Use Windows Task Scheduler to disable or delete all unnecessary and intrusive scheduled tasks
- Download and use Sysinternals Process Explorer to shut down and disable all unnecessary processes
- Download and use Sysinternals autoruns to disable unnecessary or unsafe programs (malware)
- Use Winaero Tweaker by Sergey Tkachenko , a very comprehensive, powerful, small, and free tool to make Windows behave and to look like however you want it to. Well within reason anyway. You can't make it Win7 SP2, or what Win8 should have been. It will however give you back the control that MS took away over the years
- Synchronize with an Internet time server off (should not be necessary behind a VPN)
- Windows NCSI communication across the Internet, EnableActiveProbing OFF (registry edit)
- https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc766017(v=ws.10)?redirectedfrom=MSDN
- Paid VPN (passes IP leaks, DNS leaks and WebRTC leaks)
- Zone Alarm for firewall and AV (free version is fine)
- Norton Ghost or other software for image backups to network and/or external drives
- SpyShelter anti-keyboard logger installed
- PGP Tools for encryption and decryption
- 7-Zip for creating zip files
- eBook reader software
- Quality updated gaming router with NAT
- Wireshark to analyze packet flow install Wireshark and set it to capture from your wired or Wi-Fi network interface.

https://winaerotweaker.com

More info at:

https://www.tcw.org/lefty/Short%20Stories/Configure_-The_Windows_7_To_Work_Options.pdf

https://www.tcw.org/lefty/Short%20Stories/Configure-%20Windows%208%20To%20Work,%20Kinda.pdf

More Tools for Windows 7/8/10/11:

Winaero Tweaker (a must have)
Private WinTen
Blackbird v6
O&O ShutUp10++
WPD - Windows Privacy Dashboard
SpyShelter
W10Privacy
Privatezilla
SharpApp
Debotnet

Disable Windows 10 Tracking v3.2.3
Destroy Windows 10 Spying
Win10 Spy Disabler
DisableWinTracking
Privacy Repairer
Ashampoo AntiSpy for Windows 10
Windows Privacy Dashboard

There are about **70** known security exploits out there for Windows 7, but if you stay away from websites where you really shouldn't be, and don't fall for phishing emails, you will be fine. I have been for more than ten years now.

Windows 10/11…do not despair as they are not completely hopeless but do not use on the DW

Note: You will need some skills to do this, either achieved in the process or previously hard earned, but anything really worth doing is bound to be hard. The cost is zero in dollars, depending on what you PayPal donate to the people who wrote these programs, which I do. To experiment with, use a machine that you don't need for anything else, or install free VMware player software and install it in a virtual machine.

There is a little know version of Win 10 called LTSB (Long Term Service Branch), available from 2016-2019. It is an add-on to an SA Win10 Enterprise license which is not available to most people. It also uses an SA Enterprise key for activation. There are recent hacks, available online, for this activation process available. LTSB is primarily intended for factory machinery and for kiosks.

Note: Some software may not run on this version.

The primary features are what is **not** there:

- No Cortana
- No MS Store
- No Telemetry
- No Crappy Xaml Apps
- No Forced Updates
- No Edge Browser
- No Xbox

However, since it is still Windows 10 which is a devolved, stripped down, and perverted version of the Windows we all knew and loved since 1988, it needs some serious work to make it usable. After all, Win10 was designed primarily for Mobile and Cloud computing for phones and tablets. Apparently, no one is supposed to be using desktops or non-touchscreen laptops anymore according to Microsoft's actions.

Download an MS evaluation copy to install and play with.

This is the first thing you should do going down this path. It will not activate and will work for 90 days and then quit. Before that time, however you will have figured out if this is workable for you or not.

These downloads are from the sites listed, modifications of the following areas:

- **Classic Shell** (www.classicshell.net)
  Download, install, and configure this alternate interface to your preferences.
- **Winaero** (www.winaero.com)
  Download, install, and configure Winaero Tweaker. It is amazing on what it will let you do the reconfigure Win10. It's almost daunting how many settings it provides access to. This program reminds me of all the good software I have used over the years and we don't have now, in this silly mobile app-centric phone and cloudy world. https://winaerotweaker.com
- **Aero Glass for Win8.x** (www.glass8.eu)
  Works on Win10 based on your current version.
- **Vista Icons** (https://vista-icon-pack.en.uptodown.com/windows)
  You can play like a kid with these.
- **Vista Gadgets** (https://download.cnet.com/s/gadgets-for-windows-vista/)
  Be careful where you get these. It's best to be cautious about where you get Gadgets from. Gadgets are as powerful as they are, because they have deep access to your system. Malicious code in a Gadget can truly wreak havoc. cnet.com has been a trusted site for all downloads for many years now.

If you decide this is the right approach for you, do the following:

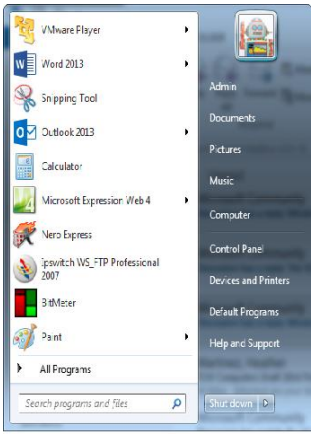
Note: I am not going to walk you through step by step with screen shots. (that would be a yet another book that I would need to sell) So some of this you will just need to figure out for yourself.

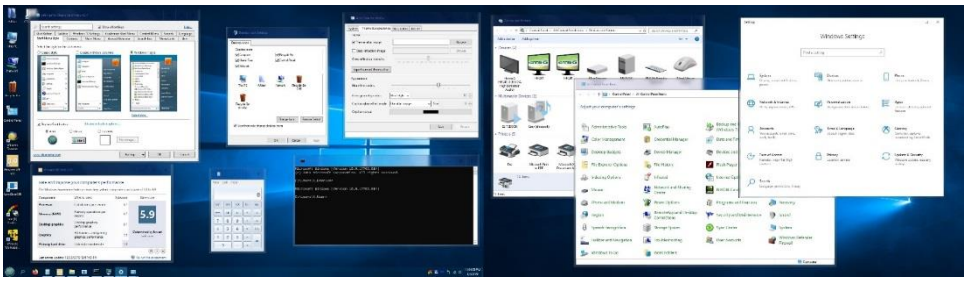
Download an available .iso and key online to a usb drive or burn to a DVD (some searching will be required to find it)
Scan the .iso with you AV and Malwarebytes
Use 7zip to unpack the .iso to a folder
Scan the unpacked .iso with AV and Malwarebytes
Install Win10 minimally
Scan your hard drive with Kaspersky rootkit finder

Once you are sure that your install is clean, you can go about reconfiguring it using the software tools as above.

Install Mozilla Firefox and some web browser extensions to keep you from getting tracked and your info stolen while on the Internet. Set the security to Strict. Use DuckDuckGo or StartPage for a search engine that doesn't track you. Use browser extensions to block ads and tracking your browsing history, and use Private Browsing on all sites. You will need to use, train, and update web browser extensions like Privacy Badger, Ghostery, DuckDuckGo Privacy Essentials, and HTTPS Everywhere to block this tracking and personal data theft.

So you can have a Start Menu that looks something like this:





You can make your system desktop look something like this, if you like.
(Dual screen setup)

More about software

The many reasons for not upgrading to Window 10/11 include the primitive interface, extensive telemetry, and the poor quality xaml software apps addressed above. One serious reason for not upgrading is software program access and compatibility. I will address this issue here. I will not address hardware compatibility, which is another valid reason.

Loss of the Media Center program is a big deal to many, even though Microsoft says that their telemetry shows that hardly anyone used it. Introduced in 2002 on Windows XP and upgraded a bit over time, it was in need of a serious upgrade to support streaming, Blu-Ray media, cable TV tuners, and many other things. This would involve not only designing and writing code, the original program development may have been outsourced, and licensing etc. Remember, Microsoft gutted their software testing department, just before the release of Win10 so the beta Win10 code could be forced on an unsuspecting public.

Microsoft is typically too far out on their skis compared to the rest of the world. They eliminated support for optical disc media early, because everyone was supposed to be using streaming like them. Unfortunately, much of the world does not have their Internet bandwidth to support this. The same is true with this continuous OS updating that strains peoples Internet accounts, not to mention many small local ISP's.

So part of this is being out of touch with reality and some of it is cost, since Windows is no longer their primary source of income and they have since moved on to all this silliness of mobile, data centers, and the illusion of secure clouds.

If you do some desktop publishing, you will notice you now have very few fonts. Typically about 300 on a Windows 7 machine and about 80 on a Win10 LTSB machine. This was another foolish move to make the OS smaller for phones and tablets, and perhaps to save money on licensing. You can get free fonts here:

https://www.1001freefonts.com/ https://www.wfonts.com/

Note: You can also get rid of the crappy App calculator by down loading and installing the old style one, and the old System Configuration and Task Manager via Winaero Tweaker.

Want to help out your fellow Internet user?

Snowflake is a system that allows people from all over the world to access censored websites and applications. Similar to how VPNs assist users in getting around Internet censorship, Snowflake helps you avoid being noticed by Internet censors by making your Internet activity appear as though you're using the Internet for a regular video or voice call. https://snowflake.torproject.org/

Help people circumvent censorship: operate a Snowflake proxy

Did you know that Snowflake proxies are operated entirely by volunteers? In other words, a user gets matched with a random Snowflake volunteer proxy, which is run by a volunteer like you! So, if you want to help people bypass censorship, consider installing and running a Snowflake proxy. The only prerequisite is that the Internet in your country is not heavily censored already.

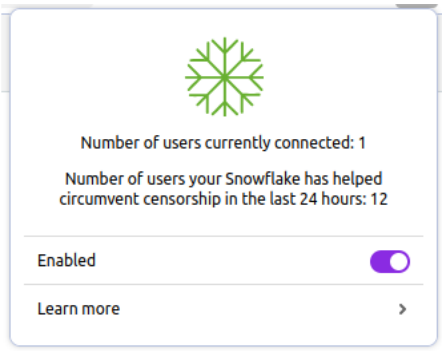
You can join thousands of volunteers from around the world who have a Snowflake proxy installed and running. There is no need to worry about which websites people are accessing through your Snowflake proxy. Their visible browsing IP address will match their Tor exit node, not yours.

There are different ways to run a Snowflake proxy (beginner to advanced):

Install the web extension

The web extension is the easiest way to run a Snowflake proxy. Simply install it on Firefox or Chrome, enable the extension, and watch the icon turn green when a user connects through your proxy!

I do, so I did.


Number of users currently connected: 1
Number of users your Snowflake has helped circumvent censorship in the last 24 hours: 12
Enabled
Learn more

This author's five novels are published on leanpub.com under the pseudonym Lefty Insider. He also publishes articles on medium.com under the same pseudonym.

The wonderful thing about the Internet is that you're connected to everyone else. The terrible thing about the Internet is that you're connected to everyone else." — Vinton Cerf, co-creator of the TCP/IP protocol

Literary Source References:

Schneier on Security
https://www.schneier.com/books/
A User's Guide to the Dark Web (and Clear Web)
(The 42nd and Final Encyclopedia Cyberspacia)
By Lefty Insider (arister0s n0stis)
https://leanpub.com/encyclopediacyberspacia
Configure The Windows 7 "To Work"
Configure Windows 8 To Work, Kind of

Postscript

It's getting worse out their people!

Yearlong Supply-Chain Attack Targeting Security Pros Steals 390,000 Credentials (arstechnica.com) 3

Posted by BeauHD on Friday December 13, 2024 @10:30PM from the unclear-motives dept.
An anonymous reader quotes a report from Ars Technica: *A sophisticated and ongoing supply-chain attack operating for the past year has been stealing sensitive login credentials from both malicious and benevolent security personnel by infecting them with Trojanized versions of open source software from GitHub and NPM, researchers said. The campaign, first reported three weeks ago by security firm Checkmarx and again on Friday by Datadog Security Labs, uses multiple avenues to infect the devices of researchers in security and other technical fields. One is through packages that have been available on open source repositories for over a year. They install a professionally developed backdoor that takes pains to conceal its presence. The unknown threat actors behind the campaign have also employed spear phishing that targets thousands of researchers who publish papers on the arXiv platform.*
The objectives of the threat actors are also multifaceted. One is the collection of SSH private keys, Amazon Web Services access keys, command histories, and other sensitive information from infected devices every 12 hours. When this post went live, dozens of machines remained infected, and an online account on Dropbox contained some 390,000 credentials for WordPress websites taken by the attackers, most likely by stealing them from fellow malicious threat actors. The malware used in the campaign also installs cryptomining software that was present on at least 68 machines as of last month. It's unclear who the threat actors are or what their motives may be. Datadog researchers have designated the group MUT-1244, with MUT short for "mysterious unattributed threat."

This is the eighth in a series of articles on Broadband Internet

An Informed Citizens View of the Current Broadband CyberSecurity Kerfuffle (Part Four)

(Why can't we make the Internet a safe place for our children, and grandchildren to live and work?)

OpSec is the term used by computer security professionals as shorthand for operational security. Keeping the bad guys from getting at your computer, or other Internet connected devices to be able to extract or exfiltrate your personal information. There are many, many, layers to this idea.

The following identifies some tools that can be used to assist you with you're your personal cybersecurity protections.

VPN's (When to use a VPN)

In a Virtual Private Network or VPN connection, an encrypted tunnel is created within an Internet connection that allows an uninterrupted flow of data from your device to a VPN server, which acts as your entry into the public Internet.

A VPN is capable of providing high speeds and it can successfully meet the needs of movie buffs and YouTubers. Remember that only your connection is encrypted and not your data, so make sure you are using the SSL (https) protocol while sending some confidential data.

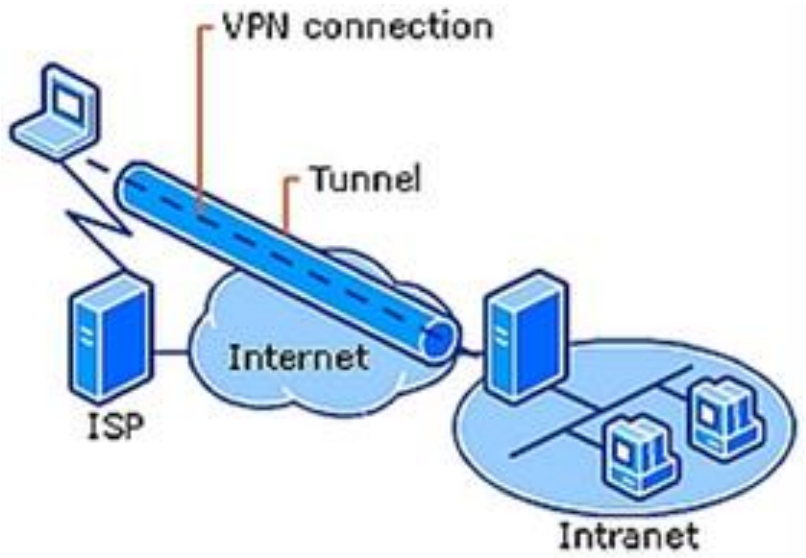
The VPN server has access to all the traffic you have initiated, popular VPN services claim that they do not store any logs. Choose a provider wisely, because that claim might be legitimate until a government agency asks them about your existence on their network.

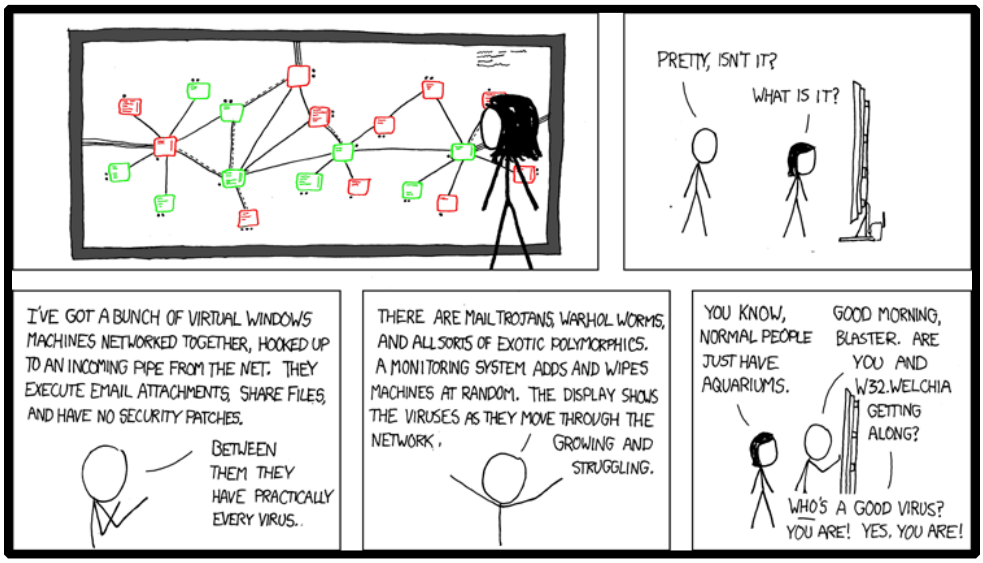
A VPN network can be used in low-risk situations like if you are not accused of some crime, or if you want to hide from various tracking tools on the Internet and simply browse the Internet or download torrents.

Sample VPN connection

VPN's are also used to extend a company's private network allowing employees to work from a remote location and still have a secure connection to the company resources.

https://www.zdnet.com/article/best-vpn/




PRETTY, ISN'T IT?
WHAT IS IT?
I'VE GOT A BUNCH OF VIRTUAL WINDOWS MACHINES NETWORKED TOGETHER, HOOKED UP TO AN INCOMING PIPE FROM THE NET. THEY EXECUTE EMAIL ATTACHMENTS, SHARE FILES, AND HAVE NO SECURITY PATCHES.
BETWEEN THEM THEY HAVE PRACTICALLY EVERY VIRUS.
THERE ARE MAIL TROJANS, WARHOL WORMS, AND ALL SORTS OF EXOTIC POLYMORPHICS. A MONITORING SYSTEM ADDS AND WIPES MACHINES AT RANDOM. THE DISPLAY SHOWS THE VIRUSES AS THEY MOVE THROUGH THE NETWORK.
GROWING AND STRUGGLING.
YOU KNOW, NORMAL PEOPLE JUST HAVE AQUARIUMS.
GOOD MORNING, BLASTER. ARE YOU AND W32.WELCHIA GETTING ALONG?
WHO'S A GOOD VIRUS? YOU ARE! YES, YOU ARE!

In a VPN connection, an encrypted tunnel is created that allows an uninterrupted flow of your data from your device to the VPN server, which acts as your entry into the public Internet.

Ten advantages of using a VPN

1. Hide your activity from your Internet Service Provider (ISP)
2. Protect yourself when using a public Wi-Fi hotspot
3. You get to keep your private searches private
4. Browse websites without leaving a trace of your identity
5. Access to streaming, wherever you are (foreign available movies)

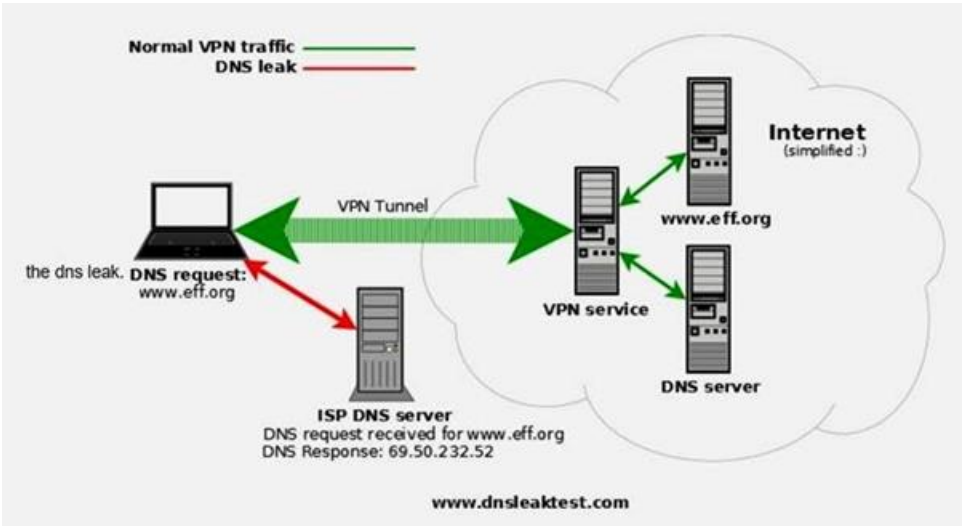
6. Stay safe from snoopers looking to access your information (most everyone)
7. Access websites not available to an IP addresses geographic location
8. Access to Internet freedom (national firewalls)
9. You can by-pass surveillance and national Internet censorship
10. You can by-pass school or workplace restrictions

UPDATE

Note: there are also browser based VPN's available, but here is what I discovered using one of them:

Ran some tests on https://routersecurity.org and discovered that the Brave browser VPN appears to leak.

Ran this same test on ExpressVPN and no leakage.



Encryption and PGP

The current lack of privacy on the Internet exposes billions of people to mass surveillance and data breaches, undermining trust in digital services and stifling innovation. Thanks to the failure of governments to ban strong encryption during the original "crypto wars" of the 1990s , open source libraries like OpenSSL created an opening for new services like PayPal, Amazon, and eBay to emerge – which would have been impossible without the end-to-end encryption between browsers and websites needed to secure financial transactions. Today is eerily similar: privacy is undermined by pervasive data collection and centralized monopolies, preventing innovative services and platforms from arising.

https://nymtech.net

In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor.

https://en.wikipedia.org/wiki/Encryption

Initially, encrypting messages required using the same tool to encrypt and decrypt making distant messaging difficult or impossible.

Two MIT mathematicians called Whitfield Diffie and Martin Hellman solved this in 1976 with a system they called “public key encryption.” Each user is given his own personal cypher system comprised of two “keys,” which are different but mathematically related to each other through their relationship to a shared prime number.

The mathematics behind it is complicated, but the idea is simple. It means you can share your “public” key with everyone, and can use it to encrypt a message into a meaningless jumble that can be decrypted only with your secret “private” key.

Public key encryption transformed the potential uses of encryption, because suddenly people were able to send encrypted messages to each other without having to exchange a code, and indeed without even having to ever meet at all.

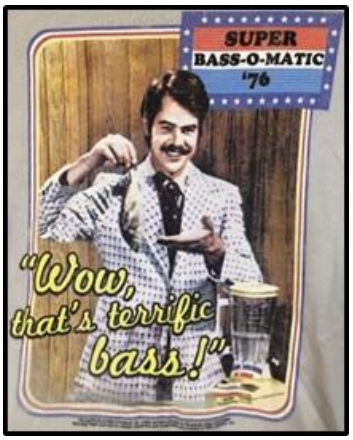
Up until the early nineties, powerful encryption was the sole preserve of governments. The United States had even classed powerful encryption as a “munition” in 1976 and made its export illegal without a license.

There are many different software programs now you can use to encrypt. This is the story of one from an excerpt from one of my previous books, The Insider (A Life Inside the Personal Computer).

Cryptology pioneer Phil Zimmermann

Phil Zimmermann was the creator of Pretty Good Privacy PGP. Phil wrote the popular Pretty Good Privacy or PGP program, made available including its source code, through public FTP[1] for downloading. This was the first widely available program to implement public-key cryptography. Shortly thereafter, the software spread uncontrollably via the new wide availability of the Internet.

The first PGP version included an encryption algorithm[2] developed by Zimmermann; that he called Bass-O-Matic with a cultural reference.



The SNL Bass-O-Matic

After a report from RSA Data Security, Inc., in a licensing dispute regarding use of the RSA algorithm2 in PGP, the United States Customs Service initiated a criminal investigation of Zimmermann, for allegedly violating the Arms Export Control Act. The United States Government regarded cryptographic software as a munition, and thus was subject to arms trafficking export controls. At that time, the boundary between cryptography permitted "low-strength" and cryptography impermissible "high-strength" for export from the United States; put PGP on the too-strong-to-export side of that boundary. The investigation lasted three years and pretty much destroyed Phil financially and emotionally for a time, but then the case was dropped without the filing of any charges. The boundary for legal export of software was later raised, and now allows PGP to be exported.

---

[1] *The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network.*

[2] *An algorithm is a self-contained sequence of actions. Software algorithms perform calculations, data processing and automated reasoning tasks.*

The government dropped its case without indictment in early 1996, and Zimmermann founded PGP Inc. to release an updated PGP version. After acquisition by Network Associates (NAI), Zimmermann stayed on as a Senior Fellow. NAI later decided to drop the product line, and PGP was reacquired from NAI by a company called the PGP Corporation. Zimmermann then served as a special advisor and consultant. Symantec later acquired the PGP Corporation. Zimmermann is a fellow at the Stanford Law School's Center for Internet and Society. He is a principal designer of the cryptographic key agreement protocol (the "association model") for the Wireless USB standard.

A 2013 article titled Zimmermann's Law, quoted Zimmermann saying, "The natural flow of technology tends to move in the direction of making surveillance easier, and the ability of computers to track us doubles every eighteen months." His words became prophetic later that year in the wake of documents released by Edward Snowden, published by Glen Greenwald and others regarding the NSA's massive surveillance of the American people and others worldwide.

https://en.wikipedia.org/wiki/Export_of_cryptography_-_from_the_United_States

This is not good.

The seven -- US, UK, Canada, Australia , New Zealand, India and Japan -- are worried that the use of end-to-end encryption makes it impossible for tech companies to identify dangerous content like terrorist propaganda and attack planning, and makes it harder for police to investigate serious crimes and protect national security.

Tech companies argue that end-to-end encryption protects users' privacy rights, and it to weaken it -- by creating a so-called 'backdoor' that would allow the authorities to look at messages -- would put all sorts of private communications at risk from hackers and force them to decide whether to hand over messages to oppressive regimes. End-to-end encryption makes the tech companies' lives easier, and also allows them to claim the moral high-ground when it comes to privacy.

https://www.zdnet.com/article/the-encryption-war-is-on-again-and-this-time-government-has-a-new-strategy/

Users adopted and tech companies introduced end-to-end encryption, due to governments incepting everyone's data and conversations in the first place. It is indeed rich that governments ask us to trust them again.

OpenPGP

PGP stands for Pretty Good Privacy. The prefix "Open" means it is open standard, so many applications support it.

OpenPGP software uses a combination of strong public-key and symmetric cryptography to provide security services for electronic communications and data storage. These services include confidentiality, key management, authentication, and digital signatures.

For those who want to know more technical details you can start with this article on the Wikipedia website. https://en.wikipedia.org/wiki/Pretty_Good_Privacy

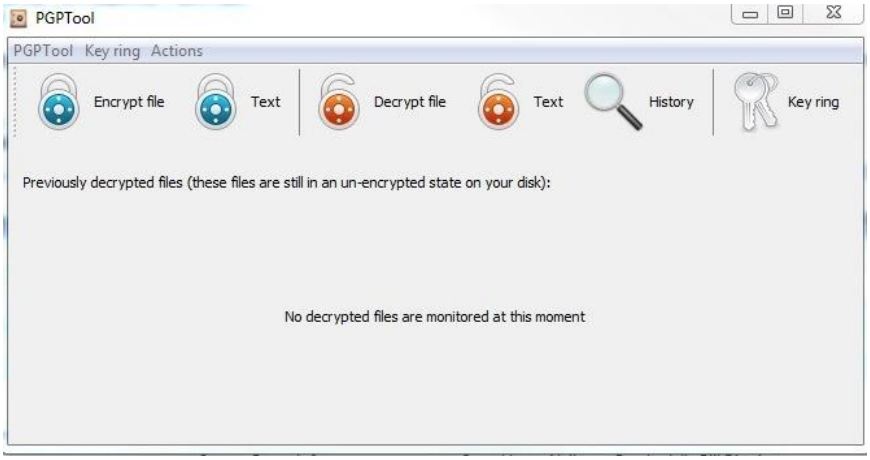
You will need a public key (PGP Global Directory).for encrypted communication. Install software and generate key.

Note: this application requires Java Runtime Environment 1.8+

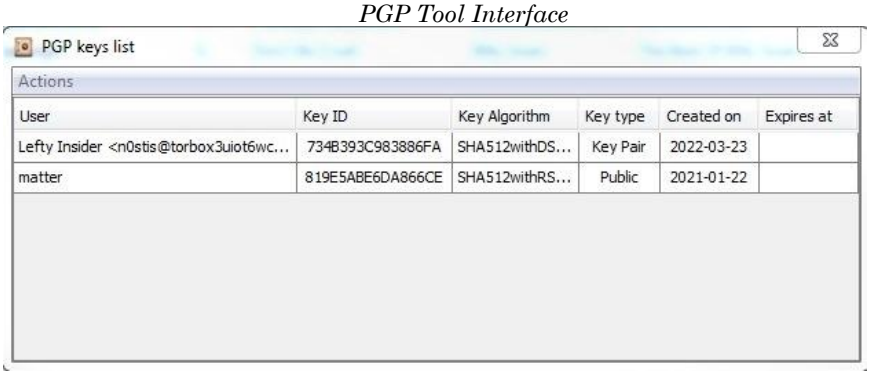
Sergey Karpushin https://www.buymeacoffee.com/skarpushind

PGP Tool and Frequently Asked Questions

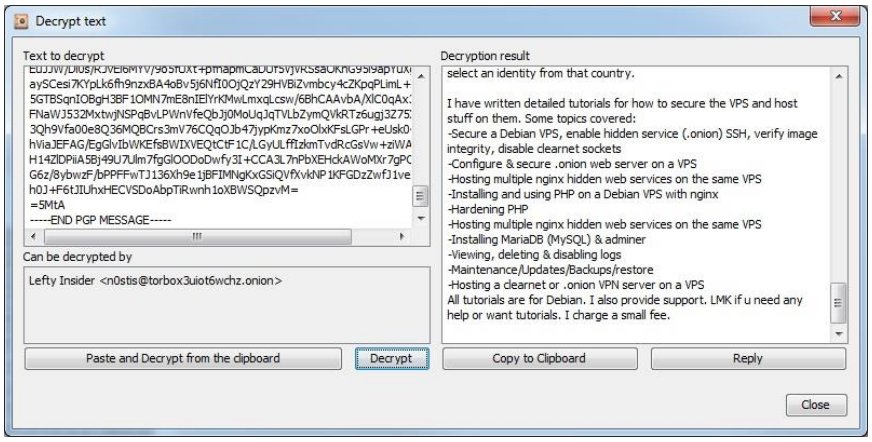
https://pgptool.github.io/#faq



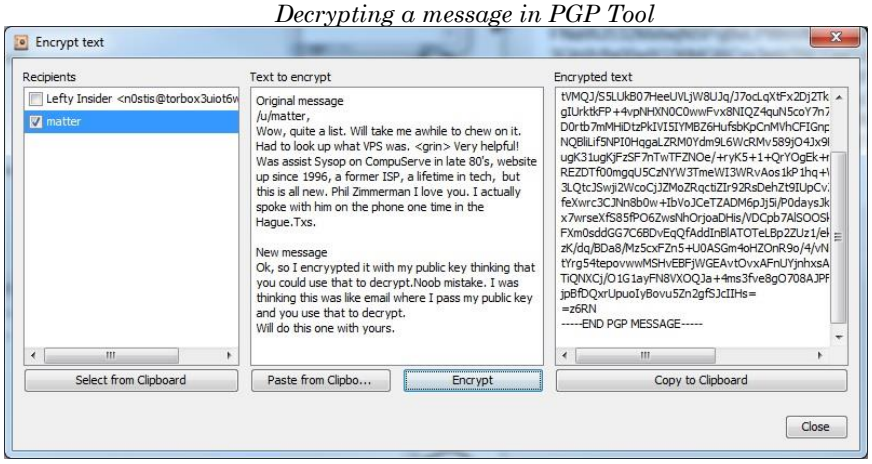
PGP Tool Interface



Select a PGP key to encrypt or decrypt with


Decrypt text
Text to decrypt
Decryption result
select an identity from that country.
I have written detailed tutorials for how to secure the VPS and host stuff on them. Some topics covered:
-Secure a Debian VPS, enable hidden service (.onion) SSH, verify image integrity, disable clearnet sockets
-Configure & secure .onion web server on a VPS
-Hosting multiple nginx hidden web services on the same VPS
-Installing and using PHP on a Debian VPS with nginx
-Hardening PHP
-Hosting multiple nginx hidden web services on the same VPS
-Installing MariaDB (MySQL) & adminer
-Viewing, deleting & disabling logs
-Maintenance/Updates/Backups/restore
-Hosting a clearnet or .onion VPN server on a VPS
All tutorials are for Debian. I also provide support. LMK if u need any help or want tutorials. I charge a small fee.
Can be decrypted by
Lefty Insider <n0stis@torbox3uiot6wchz.onion>
Paste and Decrypt from the clipboard
Decrypt
Copy to Clipboard
Reply
Close

Decrypting a message in PGP Tool


Encrypt text
Recipients
Lefty Insider <n0stis@torbox3uiot6w
matter
Text to encrypt
Original message
/u/matter,
Wow, quite a list. Will take me awhile to chew on it. Had to look up what VPS was. <grin> Very helpful! Was assist Sysop on CompuServe in late 80's, website up since 1996, a former ISP, a lifetime in tech, but this is all new. Phil Zimmerman I love you. I actually spoke with him on the phone one time in the Hague.Txs.
New message
Ok, so I encryypted it with my public key thinking that you could use that to decrypt.Noob mistake. I was thinking this was like email where I pass my public key and you use that to decrypt.
Will do this one with yours.
Encrypted text
-----END PGP MESSAGE-----
Select from Clipboard
Paste from Clipbo...
Encrypt
Copy to Clipboard
Close

Encrypting a message in PGP Tool

Note: Do not make a noob mistake and encrypt a Reply with your own key rather than the recipients key.

Annoying Advertising And What Can You Do About It?

User software like Adaware (blocks advertising on websites)

https://www.adaware.com/

Use web browser extensions with anti-trackers like:

1. DuckDuckGo Privacy Essentials (blocks tracking)
2. Ghostery (blocks trackers)
3. HTTPS Everywhere from the EFF (Electronic Frontier Foundation software that forces https secure encrypted connections), if not using Firefox or another browser with Enable **HTTPS-Only Mode in all windows** turned on
4. Privacy Badger (EFF software to block trackers) I do not use this since Firefox supports https only
5. JavaScript Restrictor (prevents malicious webpage scripts from running on your computer)

Go to your browser setting and **Manage Your Extensions (add-ons)** to add these to protect you.

Do not sign up for any tracking services or any software (apps) that may (most likely) track you. https://ssd.eff.org/en/module-categories/basics

Note: you should use a VPN that does not create log files, which may be legally subpoenaed. A free VPN might be collecting data from you, so chose your provider carefully.

Note: The NSA can store encrypted data in their datacenter in Utah, waiting for later, many years perhaps, for processing with more powerful quantum computers to beat the encryption.

Keystroke Logging and Keyloggers

Keyloggers are built for the act of keystroke logging — creating records of everything you type on a computer or mobile keyboard. These are used to quietly monitor your computer activity while you use your devices as normal. Keyloggers are used for legitimate purposes like feedback for software development, but can be misused by criminals to steal your data.

https://www.kaspersky.com/resource-center/definitions/keylogger

https://en.wikipedia.org/wiki/Keystroke_logging

Anti-keylogger Software

An anti-keylogger (or anti–keystroke logger) is a type of software specifically designed for the detection of keystroke logger software; often, such software will also incorporate the ability to delete or at least immobilize hidden keystroke logger software on a computer. In comparison to most anti-virus or anti-spyware software, the primary difference is that an anti-keylogger does not make a distinction between a legitimate keystroke-logging program and an illegitimate keystroke-logging program (such as malware); all keystroke-logging programs are flagged and optionally removed, whether they appear to be legitimate keystroke-logging software or not. The anti-keylogger is efficient in managing malicious users. It can detect the keyloggers and terminate them from the system.

https://en.wikipedia.org/wiki/Anti-keylogger

One such software available is the free version of SpyShelter. It runs in the background as a tray icon in Windows.

https://www.spyshelter.com/

Browser Fingerprinting

(AKA, a Violation of Your Privacy)

Definition:

A device fingerprint or machine fingerprint is information collected about the software and hardware of a remote computing device for the purpose of identification. The information is usually assimilated into a brief identifier using a fingerprinting algorithm. A browser fingerprint is information collected specifically by interaction with the web browser of the device.

Device fingerprints can be used to fully or partially identify individual devices even when persistent cookies (and zombie cookies) cannot be read or stored in the browser, the client IP address is hidden, or one switches to another browser on the same device. This may allow a service provider to detect and prevent identity theft and credit card fraud, but also to compile long-term records of individuals' browsing histories (and deliver targeted advertising) or targeted exploits even when they are attempting to avoid tracking – raising a major concern for Internet privacy advocates.

https://en.wikipedia.org/wiki/Device_fingerprint

How does online fingerprint identify me?

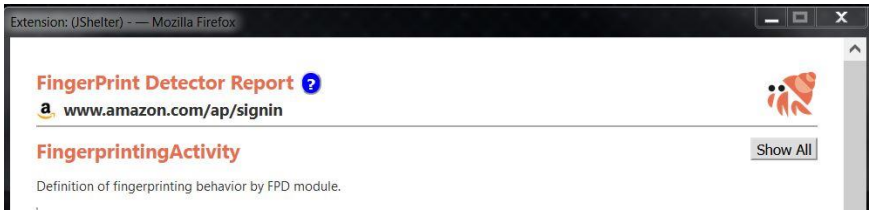
With browser fingerprints, the information collected about you includes numerous data points that predominantly help track the following details:

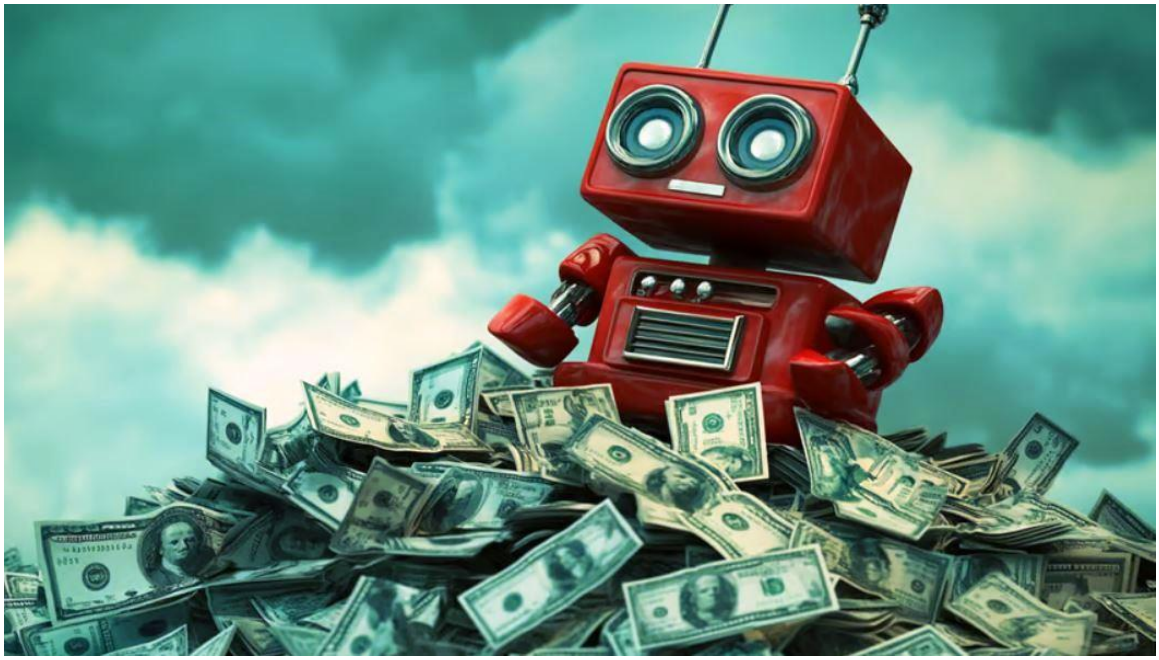
1. Type of browser and version
2. Browser settings
3. Active plugins
4. IP address
5. Device Operating System
6. Device type and model
7. Network type (or ISP)
8. Device time zone
9. Users' location
10. Language
11. Screen resolution
12. Active JavaScript
13. Active Flash

Note: Use Firefox JShelter JavaScript shield to prevent fingerprinting

FingerPrint Detector Report

This report lists all JavaScript API endpoints that were accessed by the web page and are considered critical in terms of browser fingerprinting. Fingerprint Detector (FPD) uses this data to decide whether the page is collecting a browser fingerprint.





These data collections are corporate decisions made to harvest this data from unsuspecting website visitors. This is just more of the current corporate vulture capitalism at work, as if a giant squid wrapped itself around the Internet, sticking its tentacles into anything and everything to suck out, harvest, and process, any and all, information that they can somehow turn into money.

Some people block their browser cookies, so they respond in turn by doing this fingerprinting. No one consensually agreed, nor were asked to allow this kind of unsolicited and unremunerated privacy intrusion.

The Firefox web browser warns you about this. Apple Safari, Microsoft Edge, and Google Chrome, will not because they are part of the problem. If you turn off JavaScript[3] and Flash, and add a privacy browser extension, you may be able to thwart these privacy intrusions with these corporate browsers.

There is very good information and advice on this here:

https://privacysavvy.com

https://privacysavvy.com/security/safe-browsing/browser-fingerprinting/

[3] This may cause problems with lots of websites, so bookmark your preferences page in your browser, i.e. in Firefox about:config.

Acceptable Browser results

Our tests indicate that you have you have strong protection against Web tracking, though your software isn't checking for Do Not Track policies.
IS YOUR BROWSER:
Blocking tracking ads? Yes
Blocking invisible trackers? Yes
Protecting you from fingerprinting? Yes

This is what your test should look like.

https://www.wikihow.com/Disable-JavaScript

Notes:

1. **You cannot disable JavaScript in the iPhone or iPad version of Firefox**
2. **You cannot disable JavaScript in the iPhone or iPad version of Chrome**
3. **When you update Google Chrome, you may have to re-disable JavaScript**
4. **You may have to re-disable JavaScript after you update your iPhone**
5. **When you update the Firefox app, you may need to disable JavaScript again**

And all of this tells you somethings right there.

Note: Disabling JavaScript is also a quick way to load content-rich websites when on a slow Internet connection.

This author's five novels are published on leanpub.com under the pseudonym Lefty Insider. He also publishes articles on medium.com under the same pseudonym.

"Those who would give up an essential liberty for temporary security deserve neither liberty nor security." -- Benjamin Franklin

Literary Source References:

Schneier on Security
https://www.schneier.com/books/
A User's Guide to the Dark Web (and Clear Web)
(The 42nd and Final Encyclopedia Cyberspacia)
By Lefty Insider (arister0s n0stis)
https://leanpub.com/encyclopediacyberspacia

Postscript

It's getting worse out there people!

Hackers hit Rhode Island benefits system in major cyber-attack. Personal data could be released soon https://apnews.com/article/cybersecurity-breach-data-rhode-island-56875d6b20ce94de7b240c5b2f43e4a8

Hackers Hit Rhode Island Benefits System In Major Cyberattack (apnews.com) 24

Posted by BeauHD on Monday December 16, 2024 @06:40PM from the **another-day-another-breach dept.**

A cyberattack on Rhode Island's RIBridges system has exposed personal data of individuals involved in programs like Medicaid, SNAP, and others, with hackers demanding a ransom. The breach may include sensitive details like Social Security numbers and banking information. The Associated Press reports: *Anyone who has been involved in Medicaid, the Supplemental Nutrition Assistance Program known as SNAP, Temporary Assistance for Needy Families, Childcare Assistance Program, Rhode Island Works, Long-term Services and Supports, the At HOME Cost Share Program and health insurance purchased through HealthSource RI may be impacted, McKee said Saturday.*

The system known as RIBridges was taken offline on Friday, after the state was informed by its vendor, Deloitte, that there was a major security threat to the system. The vendor confirmed that "there is a high probability that a cybercriminal has obtained files with personally identifiable information from RIBridges," the state said. The state has contracted with Experian to run a toll-free hotline for Rhode Islanders to call to get information about the breach and how they can protect their data.

Was the US Telecom Breach Inevitable, Proving Backdoors Can't Be Secure? (theintercept.com) 47

Posted by EditorDavid on Saturday December 14, 2024 @09:34PM from the too-big-for-your-breaches dept.

America's 1994 "Communications Assistance for Law Enforcement Act" (or CALEA) created the security hole that helped enable a massive telecomm breach. But now America's FBI "is falling back on the same warmed-over, bad advice about encryption that it has trotted out for years," argues the Intercept: *In response to the Salt Typhoon hack, attributed to state-backed hackers from China, the bureau is touting the long-debunked idea that federal agents could access U.S. communications without opening the door to foreign hackers. Critics say the FBI's idea, which it calls "responsibly managed encryption," is nothing more than a rebranding of a government backdoor. "It's not this huge about-face by law enforcement," said Andrew Crocker, the surveillance litigation director at the Electronic Frontier Foundation. "It's just the same, illogical talking points they have had for 30+ years, where they say, 'Encryption is OK, but we need to be able to access communications.' That is a circle that cannot be squared...."*

In a blog post last month, encryption expert Susan Landau said CALEA had long been a "national security disaster waiting to happen... If you build a system so that it is easy to break into, people will do so — both the good guys and the bad. That's the inevitable consequence of CALEA, one we warned would come to pass — and it did," she said...
Sean Vitka, the policy director at the progressive group Demand Progress, said the hack has once again provided damning evidence that government backdoors cannot be secured. "If the FBI cannot keep their wiretap system safe, they absolutely cannot keep the skeleton key to all Apple phones safe," Vitka said.

US Government Tells Officials, Politicians To Ditch Regular Calls and Texts (reuters.com) 36

Posted by msmash on Wednesday December 18, 2024 @03:00PM from the breaking-news dept.

The U.S. government is urging senior government officials and politicians to ditch phone calls and text messages following intrusions at major American telecommunications companies blamed on Chinese hackers. From a report: *In written guidance, opens new tab released on Wednesday, the Cybersecurity and Infrastructure Security Agency said "individuals who are in senior government or senior political positions" should "immediately review and apply" a series of best practices around the use of mobile devices.*
The first recommendation: "Use only end-to-end encrypted communications." End-to-end encryption -- a data protection technique which aims to make data unreadable by anyone except its sender and its recipient -- is baked into various chat apps, including Meta's WhatsApp, Apple's iMessage, and the privacy-focused app Signal. Neither regular phone calls nor text messages are end-to-end encrypted, which means they can be monitored, either by the telephone companies, law enforcement, or - potentially - hackers who've broken into the phone companies' infrastructure.

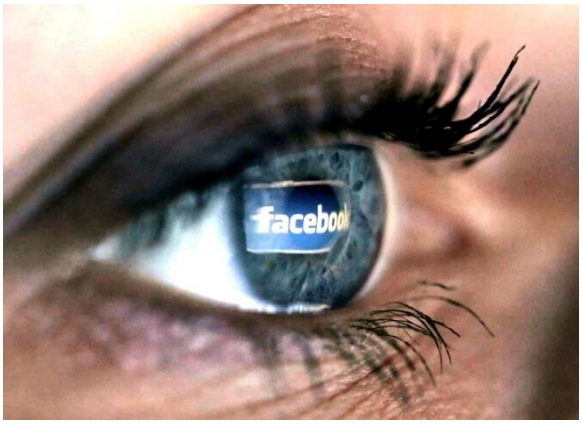
This is the ninth in a series of articles on Broadband Internet

An Informed Citizens View of the Current Broadband CyberSecurity Kerfuffle (Part Five)

(Why can't we make the Internet a safe place for our children, and grandchildren to live and work?)

OpSec is the term used by computer security professionals as shorthand for operational security. Keeping the bad guys from getting at your computer, or other Internet connected devices to be able to extract or exfiltrate your personal information. There are many, many, layers to this idea.

The following identifies information that can be used to assist you with cybersecurity knowledge, your personal information protection, and device hygiene.



What data Facebook (Meta) collects

For those who have the somewhat naïve view that they have nothing to hide, below is a sample of what just Facebook alone collects:

Targeting options for Facebook advertisers

1. Location, via GPS or if turned off, via local cell towers
2. Age
3. Generation
4. Gender
5. Language
6. Education level

7. Field of study
8. School
9. Ethnic affinity
10. Income and net worth
11. Home ownership and type
12. Home value
13. Property size
14. Square footage of home
15. Year home was built
16. Household composition
17. Users who have an anniversary within 30 days
18. Users who are away from family or hometown
19. Users who are friends with someone who has an anniversary, is newly married, or engaged, recently moved, or has an upcoming birthday
20. Users in long-distance relationships
21. Users in new relationships
22. Users who have new jobs
23. Users who are newly engaged
24. Users who are newly married
25. Users who have recently moved
26. Users who have birthdays soon
27. Parents
28. Expectant parents
29. Mothers divided by "type" (soccer, trendy, etc.)
30. Users who are likely to engage in politics
31. Conservatives and liberals
32. Relationship status
33. Employer
34. Industry
35. Job title
36. Office type
37. Interests
38. Users who own motorcycles
39. Users who plan to buy a car (and what kind/brand of car, and how soon)
40. Users who bought auto parts or accessories recently
41. Users who are likely to need auto parts or services
42. Style and brand of car you drive
43. Year car was bought
44. Age of car
45. How much money user is likely to spend on next car?
46. Where user is likely to buy next car
47. How many employees your company has
48. Users who own small businesses
49. Users who work in management or are executives
50. Users who have donated to charity (divided by type)
51. Operating system on your computer
52. Users who play canvas games
53. Users who own a gaming console
54. Users who have created a Facebook event

55. Users who have used Facebook Payments
56. Users who have spent more than average on Facebook Payments
57. Users who administer a Facebook page
58. Users who have recently uploaded photos to Facebook
59. Internet browser
60. Email service
61. Early/late adopters of technology
62. Expats (divided by country they are from originally)
63. Users who belong to a credit union, national bank, or regional bank
64. Users who investor (divided by investment type)
65. Number of credit lines
66. Users who are active credit card users
67. Credit card type
68. Users who have a debit card
69. Users who carry a balance on their credit card
70. Users who listen to the radio
71. Preference in TV shows
72. Users who use a mobile device (divided by brand)
73. Internet connection type
74. Users who recently acquired a smartphone or tablet
75. Users who access the Internet via a smartphone or tablet
76. Users who use coupons
77. Types of clothing user's household buys
78. Time of year user's household shops most
79. Users who are "heavy" buyers of beer, wine, or spirits
80. Users who buy groceries (and what kinds)
81. Users who buy beauty products
82. Users who buy allergy medications, cough/cold medications, pain relief products, and over-the-counter meds
83. Users who spend money on household products
84. Users who spend money on products for kids or pets, and what kinds of pets
85. Users whose household makes more purchases than is average
86. Users who tend to shop online (or off)
87. Types of restaurants user eats at
88. Kinds of stores user shops at
89. Users who are "receptive" to offers from online auto insurance, higher education, or mortgages and prepaid debit cards/satellite TV
90. Length of time user has lived in house
91. Users who are likely to move soon
92. Users who are interested in the Olympics, fall football, cricket, or Ramadan
93. Users who travel frequently, for work or pleasure
94. Users who commute to work
95. Types of vacations user tends to go on
96. Users who recently returned from a trip
97. Users who recently used a travel app
98. Users who participate in a timeshare

Does anyone think that this is creepy, or worrisome?

Delete your Facebook account

Did you know that a small sample of a hundred plus items that Facebook alone collects about you includes:

User income and net worth, user affiliations with credit unions, national banks or regional banks, your preferences in TV shows, users who are "heavy" buyers of beer, wine or spirits, users who are "receptive" to offers from companies offering online auto insurance, higher education or mortgages, and prepaid debit cards/satellite TV?

It is well documented in both books and legislative testimony that the British company Cambridge Analytical turned the military-grade psychological warfare techniques developed to deter ISIS recruitment, against the American voters. These were specifically targeted short-lived Facebook ads used to change opinions and prey on the uninformed and naïve among us. Facebook has been unwilling to this point to share the content of these ads.

In addition, Russian Facebook ads, based on Republican polling data individually targeted Facebook users and spread false narratives to create division among us.

Now for sure, Facebook will track your activities across the Internet even if you do not have a Facebook account. You will need to use web browser extensions like Privacy Badger, Ghostery, and HTTPS Everywhere to block this tracking.

Whatever perceived or real value comes from the use of this social network pales in comparison to the damage caused by fomenting division among us, and to never, ever, being able to have a free and fair election again in this country. It is now past the time to show your patriotism as an American, delete your Facebook account, and then continue to protect yourself on the Internet.

1/4/20 Fresh Cambridge Analytica leak 'shows global manipulation is out of control'

Company's work in 68 countries releases more than 100,000 documents

An explosive leak of tens of thousands of documents from the defunct data firm Cambridge Analytica is set to expose the inner workings of the company that collapsed after the Observer revealed it had misappropriated 87 million Facebook profiles.

More than 100,000 documents relating to work in 68 countries that will lay bare the global infrastructure of an operation used to manipulate voters on "an industrial scale" is set to be released over the next months.

It comes as Christopher Steele, the ex-head of MI6's Russia desk and the intelligence expert behind the so-called "Steele dossier" into Trump's relationship with Russia, said that while the company had closed down, the failure to properly punish bad actors meant that the prospects for manipulation of the US election this year were even worse.

- https://www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation

Hundreds of Millions of Facebook Users Data Exposed

Information could be deployed for spam or phishing attacks

Information on 267 million Facebook users, including user names, phone numbers and Facebook IDs, was exposed online, according to a cybersecurity researcher.

The data, mostly from U.S. Facebook users, was posted on a searchable database by a group that appeared to be based in Vietnam, said Bob Diachenko, the cyber threat intelligence director at Security Discovery, a Ukrainian cybersecurity website that offers news and consulting services. The Vietnamese group appeared to be charging for access to the data, but a flaw in their code inadvertently left the database open to all, he said.

- https://www.bloomberg.com/news/articles/2019-12-20/data-on-hundreds-of-millions-of-u-s-facebook-users-exposed?srnd=technology-vp

Facebook offers funny answer for why it tracks users' locations even when they turn tracking services off

Facebook offered a revealing explanation to lawmakers for why it continues to track users' locations even after those users turn Facebook's location tracking services off.

Responding to a letter from Sen. Josh Hawley, (R-MO), and Sen. Chris Coons, (D-DE), Facebook said it needs that extra location data to target ads, and for various security functions. The two senators asked Facebook last month to "respect" users' decisions to keep their locations private. Coons and Hawley now say that Facebook needs to give users more control over their data. I say, just go ahead and delete Facebook.

- https://boingboing.net/2019/12/18/facebook-offers-funny-answer-f.html

1/13/20 Facebook Exec Says Company Helped Elect Trump And May Just Do It Again

Facebook Vice President Andrew Bosworth also said that the president's victory was not a result of outside influence but of clever digital advertising.

Bosworth later shared that the comments were "not meant for public consumption."

Bosworth's December remarks surfaced in reports Tuesday, a day after Trump claimed that Zuckerberg told the president during their dinner in October that he was "number 1" on the social media platform.

https://www.huffpost.com/entry/facebook-exec-company-helped-elect-trump-do-it-again_n_5e154bdcc5b6c7b859d28648

A plea to save Democracy from a reporter

Who's Afraid of the IRS? Not Facebook. (propublica.org)

In March 2008, as Facebook was speeding toward 100 million users and emerging as the next big tech company, it announced an important hire. Sheryl Sandberg was leaving Google to become Facebook's chief operating officer. CEO Mark Zuckerberg, then 23 years old, told The New York Times that Sandberg would take the young company "to the next level." Based on her time at Google, Sandberg soon decided that one area where Facebook was behind its peers was in its tax dodging. "My experience is that by not having a European center and running everything through the US, it is very costly in terms of taxes," she wrote other executives in an April 2008 email, which has not been previously reported. Facebook's head of tax agreed, replying that the company needed to find "a low taxed jurisdiction to park profits." Later that year, Facebook named Dublin as its international headquarters, just as Google had done when Sandberg was there. And just like Google, Facebook concocted an intra-company deal to "park profits" in Ireland, where it would pay a tax rate near zero.

Like its Big Tech peers, Facebook wasn't much afraid of the IRS. But, as it happened, the same year that Facebook started moving profits to Ireland, the IRS launched a team to crack down on deals like that. The effort started aggressively. As we recently reported, the IRS threw everything it had at Microsoft in the largest audit in the agency's history. But shortly after the IRS showed this new ambition, Republicans in Congress, after taking the House in 2010, began forcing cuts to the IRS' budget. Over the years, as Facebook grew into one of the world's largest companies, with 2 billion users, the IRS was shrinking. By the time the IRS finally took on Facebook over its Irish deal a few years later, the agency was in over its head. ProPublica pieced together the story of the Facebook audit from court documents filed by the two sides in their years long battle. The picture revealed by the documents provides a crucial window into the IRS' struggles to check large corporations' tax schemes.

Facebook To Pay $550 Million To Settle Facial Recognition Suit (nbcnews.com)

Facebook has agreed to pay $550 million to settle a class-action lawsuit (Warning: source may be pay walled; alternative source) over its use of facial recognition technology in Illinois, "giving privacy groups a major victory that again raised questions about the social network's data-mining practices," reports The New York Times. From the report: The case stemmed from Facebook's photo-labeling service, Tag Suggestions, which uses face-matching software to suggest the names of people in users' photos. The suit said the Silicon Valley company violated an Illinois biometric privacy law by harvesting facial data for Tag Suggestions from the photos of millions of users in the state without their permission and without telling them, how long the data would be kept. Facebook has said the allegations have no merit. Under the agreement, Facebook will pay $550 million to eligible Illinois users and for the plaintiffs' legal fees.

More reading and viewing:

Meet Brittany Kaiser, Cambridge Analytica Whistleblower Releasing Troves of New Files from Data Firm (six part series)

https://www.democracynow.org/2020/1/7/the_great_-hack_cambridge_analytica

Zucked: Early Facebook Investor Roger McNamee on How the Company Became a Threat to Democracy (four part series)

https://www.democracynow.org/2019/10/23/roger_-mcnamee_zucked_facebook_mark_zuckerberg

Roger McNamee singles out Facebook and Google for their roles in spreading disinformation.

https://finance.yahoo.com/news/roger-mcnamee-on-climate-change-anti-vaxxing-white-supremacy-120859801.html

Facebook Doesn't Know What It Does With Your Data, Or Where It Goes (vice.com) 26

Posted by BeauHD on Wednesday April 27, 2022 @06:00AM from the surprise-surprise dept.

em1ly shares a report from Motherboard: Facebook is facing what it describes internally as a "tsunami" of privacy regulations all over the world, which will force the company to dramatically change how it deals with users' personal data. And the "fundamental" problem, the company admits, is that Facebook has no idea where all of its user data goes, or what it's doing with it, according to a leaked internal document obtained by Motherboard. "We've built systems with open borders. The result of these open systems and open culture is well described with an analogy: Imagine you hold a bottle of ink in your hand. This bottle of ink is a mixture of all kinds of user data (3PD, 1PD, SCD, Europe, etc.) You pour that ink into a lake of water (our open data systems; our open culture) ... and it flows ... everywhere," the document read. "How do you put that ink back in the bottle? How do you organize it

again, such that it only flows to the allowed places in the lake?" (3PD means third-party data; 1PD means first-party data; SCD means sensitive categories data.)

The document was written last year by Facebook privacy engineers on the Ad and Business Product team, whose mission is "to make meaningful connections between people and businesses," and which "sits at the center of our monetization strategy and is the engine that powers Facebook's growth," according to a recent job listing that describes the team. This is the team that is tasked with building and maintaining Facebook's sprawling ads system, the core of the company's business. And in this document, the team is both sounding an alarm, and making a call to change how Facebook deals with users' data to prevent the company from running into trouble with regulators in Europe, the US, India, and other countries that are pushing for more stringent privacy constraints on social media companies. "We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.' And yet, this is exactly what regulators expect us to do, increasing our risk of mistakes and misrepresentation," the document read. In other words, even Facebook's own engineers admit that they are struggling to make sense and keep track of where user data goes once it's inside Facebook's systems, according to the document. This problem inside Facebook is known as "data lineage."

Then if you haven't already read enough. The reasons given below to use this tool are the exact same reasons that you should not allow this tool to be used against you and your privacy rights.

Facebook Pixel: What It Is and Why You Need It

If your business advertises on Facebook, you should already know about the Facebook pixel. This code will optimize your Facebook ad strategy and help you make the most of your advertising budget. The Facebook pixel helps you reach new, relevant audiences and track their engagement with your ads.

What Is a Facebook Pixel?

The Facebook pixel is a short piece of code that businesses can add to their website to track their Facebook ad campaigns. The pixel measures ad conversions, website traffic, and monitors audiences.

The Facebook pixel also helps you to create custom audiences for your Facebook ads, allowing you to target certain demographics and retarget customers or visitors to your website.

How Does Facebook Pixel Work?

When a customer takes action on your website, the Facebook pixel code is triggered and reports their actions. The report of your Facebook pixel activity can be found in Facebook's ads manager.

The pixel tracks customer journeys through your website and reveals whether they completed your desired action, whether it's buying a product, subscribing, or filling out a form.

Learning customer data and how they engage with your website and with advertisements can help you focus your target audience, retarget custom audiences, and improve your ads. The Facebook pixel helps you optimize your ads to increase customer conversions.

Facebook Pixel Cost

Installing the Facebook pixel is totally free! Advertising on Facebook is not free, of course, but setting up the Facebook tracking pixel is free. The Facebook pixel will even save you money spent on advertising, as you can get more out of your ads.

Why You Need The Facebook Pixel

The Facebook pixel helps businesses track and optimize their Facebook ads. If you're advertising on Facebook, you should absolutely install the Facebook pixel so that you better understand how your ads perform.

Tracking the Facebook pixel allows you to place your ads in front of the best possible audience, leading to better conversion rates and ROIand ROAS for your ad budget.

Keep reading to learn all the ways that the Facebook pixel can benefit your social media marketing strategy.

https://seodigitalgroup.com/facebook-pixel/

DC Attorney General Sues Mark Zuckerberg Over Cambridge Analytica Data Breach (go.com) 39

Posted by BeauHD on Monday May 23, 2022 @06:00PM from the personally-involved dept.

An anonymous reader quotes a report from ABC News: Washington, D.C., Attorney General Karl Racine has sued Meta CEO Mark Zuckerberg for allegedly failing to protect consumer data following the Cambridge Analytica data leak. "The evidence shows Mr. Zuckerberg was personally involved in Facebook's failure to protect the privacy and data of its users leading directly to the Cambridge Analytica incident," Racine said in a statement about the lawsuit released Monday. "This unprecedented security breach exposed tens of millions of Americans' personal information, and Mr. Zuckerberg's policies enabled a multi-year effort to mislead users about the extent of Facebook's wrongful conduct." He added, "This lawsuit is not only warranted, but necessary, and sends a message that corporate leaders, including CEOs, will be held accountable for their actions."

The lawsuit alleges that Zuckerberg was "responsible for" and "had the clear ability" to control Facebook operations and enabled Cambridge Analytica to use consumer data. The lawsuit alleges that third-party firms like Cambridge Analytica got data from 87 million Americans and half of District of Columbia residents. Racine filed a lawsuit against Facebook in December 2018 for the data leak and is bringing this suit following evidence found during that litigation, according to the attorney general. In March, a judge ruled against an effort by Racine to add Zuckerberg as a defendant in the ongoing 2018 case. [...] The lawsuit filed by Racine takes issue with what it appears to consider a central business objective of Facebook. The suit accuses the company of aiming "to convince people to reveal the most granular details of

who they are to Facebook -- their religions, their work histories, their likes -- so that it can be monetized, and Zuckerberg and his company can continue to grow even wealthier." On multiple occasions, the lawsuit notes that the company pursued its policies "at Zuckerberg's direction."

Report: Facebook has Started Encrypting Links to Counter Browsers' Anti-Tracking Measures (ghacks.net) 74

Posted by EditorDavid on Monday July 18, 2022 @07:34AM from the whose-link-is-it-anyway? dept.

"Facebook has started to use a different URL scheme for site links," writes the technology blog Ghacks, "to combat URL stripping technologies that browsers such as Firefox or Brave use to improve privacy and prevent user tracking." Some sites, including Facebook, add parameters to the web address for tracking purposes. These parameters have no functionality that is relevant to the user, but sites rely on them to track users across pages and properties. Mozilla introduced support for URL stripping in Firefox 102, which it launched in June 2022. Firefox removes tracking parameters from web addresses automatically, but only in private browsing mode or when the browser's Tracking Protection feature is set to strict. Firefox users may enable URL stripping in all Firefox modes, but this requires manual configuration. Brave Browser strips known tracking parameters from web addresses as well....

It is no longer possible to remove the tracking part of the URL, as Facebook merged it with part of the required web address.

Zuckerberg and Sandberg Ordered To Testify Over Alleged Involvement In Cambridge Analytica Scandal (gizmodo.com) 23

Posted by BeauHD on Wednesday July 20, 2022 from the time-to-face-the-music dept.

An anonymous reader quotes a report from Gizmodo: Meta CEO Mark Zuckerberg and former COO Sheryl Sandberg will have to provide testimony to a federal court to discuss their alleged involvement in the company's notorious Cambridge Analytica scandal, over half a decade since it first captured the world's attention. [...] Cambridge Analytica was a British political consulting firm that used Facebook user data to target and lobby potential voters ahead of the 2016 election in favor of Donald Trump. The ensuing scandal helped trigger an investigation from the Federal Trade Commission that resulted in Facebook agreeing to a record-setting $5 billion settlement over its privacy practices.

A new filing (PDF) in the Northern District of California Tuesday shows Zuckerberg and Sandberg agreed to be deposed for six and five hours respectively in September of this year. This comes as part of a class action lawsuit filed against Meta, claiming the company violated consumer privacy laws when it shared user data with Cambridge Analytica back in 2015. [...] In addition to Zuckerberg and Sandberg, the court's also seeking to depose Meta's newly named CTO Javier Olivan -- who previously served as the company's Chief Growth Officer -- as well as a handful of other "key witnesses." Olivan's deposition is expected to last three hours. According to Tuesday's filing Meta will also hand over 1,200 documents "previously withheld as privileged." Plaintiffs in the case previously accused Meta and the law firm representing it of "stonewalling," during the court's discovery phase.

More Than 140 Kenya Facebook Moderators Diagnosed With Severe PTSD (theguardian.com) 42

Posted by BeauHD on Tuesday December 24, 2024 @07:02PM from the human-cost-of-moderation dept.

An anonymous reader quotes a report from The Guardian: *More than 140 Facebook content moderators have been diagnosed with severe post-traumatic stress disorder caused by exposure to graphic social media content including murders, suicides, child sexual abuse and terrorism. The moderators worked eight- to 10-hour days at a facility in Kenya for a company contracted by the social media firm and were found to have PTSD, generalized anxiety disorder (GAD) and major depressive disorder (MDD), by Dr Ian Kanyanya, the head of mental health services at Kenyatta National hospital in Nairobi. The mass diagnoses have been made as part of lawsuit being brought against Facebook's parent company, Meta, and Samasource Kenya, an outsourcing company that carried out content moderation for Meta using workers from across Africa.*

The images and videos including necrophilia, bestiality and self-harm caused some moderators to faint, vomit, scream and run away from their desks, the filings allege. The case is shedding light on the human cost of the boom in social media use in recent years that has required more and more moderation, often in some of the poorest parts of the world, to protect users from the worst material that some people post. The lawsuit claims that at least 40 moderators experienced substance misuse, marital breakdowns, and disconnection from their families, while some feared being hunted by terrorist groups they monitored. Despite being paid eight times less than their U.S. counterparts, moderators worked under intense surveillance in harsh, warehouse-like conditions.

Stop using Google

The Internet was purposely designed with its intelligence, like personal computers and other connecting devices, only at the end points. More specifically, it was designed as a democratic system with no centralized computer control of access, or data collection. This design was mostly a reaction to the perceived centralized fascistic operation of the prior mainframe computer era and its dumb terminals for computer users.

Now these unbridled capitalist digital gangster corporations like Google, have inserted themselves as Internet gateways into every transaction and communication across your Internet. They have, without your express permission, exerted *Eminent Domain* over your personal data. They refer to this data as digital exhaust, a euphemism to obfuscate and diminish this theft. Google alone (10 million servers headed for 100 million) collects a staggering amount of data and stores it forever. More than 500 megabytes per person per day. By way of comparison, this letter as an MS Word document equals about 0.3% of that amount of daily collected personal data.

4.62 billion pages indexed by Google as of May 2016, according to WorldWideWebSize
Almost 148 million domains or unique websites, as estimated by

DomainTools
More than 3.5 billion Google searches covering more than 20 billion sites every day, as reported by Internet Live Stats

New York (CNN Business) Google has confirmed its collecting health data on millions of Americans through a new partnership with Ascension, one of the country's largest nonprofit health systems. The project is codenamed "Project Nightingale," although this revelation is light on specifics, Google and Ascension said the partnership would integrate Ascension's various silos of health data into the cloud. (In other words, Googles server computers)

Imaging how this data might be used against you in the future, for insurance applications, college admissions, life insurance applications, or employment applications. Think of the effect on not only you, but also your children and grandchildren.

Not unlike the Truman show movie, Google is using their tools and code to record everyone's digital lives, monitoring, guiding, predicting behaviors, and make enormous profits from doing this.

What to do? Stop giving them your personal data! Use DuckDuckGo or better yet StartPage, for a search engine that does not track you. Use browser extensions to block ads and tracking your browsing history, and use Private Browsing.

Stop using the Google Chrome browser because it tracks you, the Mozilla Firefox browser does not. Do not buy or use a Chromebook, it is a surveillance tool. Do not use Alexa for the same reason. Stop using Google Docs and use Libre Office or MS Office instead. Do not use Google Maps or YouTube. Use openstreetmap.org and Vimeo.com instead. I know you like cat videos, but do it anyway. Do not use a Ring doorbell either, or other Internet connected cameras, appliances, thermostats, and baby monitors.

Amazon is facing criticism over its home security cameras called Ring, after a data leak exposed the personal information of over 3,000 users. The data breach includes emails, passwords and other sensitive information that would allow hackers to access live camera footage from inside every room of people's homes. The data breach follows criticism over Ring's cooperation with more than 400 police departments, giving cops the ability to use homeowners' camera footage in their investigations. A group of 30 civil rights groups published a joint letter demanding that lawmakers stop the police partnership, calling it a threat to civil rights and liberties, especially for black and brown communities.

- https://www.democracynow.org

Corporate abuse can be stopped, as were the 19th-century Robber Barons. Government intervention filed an antitrust case against IBM in the 1970's, broke up AT&T in the 1980's, throttled Microsoft with a consent decree in the 1990's , and fined Facebook and Google millions of dollars numerous times in the 2000's.

You should advocate for enforcement of existing laws, (Sherman Antitrust Act) and for creating data protection laws like those enacted in the European Union.

The “Don’t be Evil” slogan of an early benevolent startup company has been replaced by a malevolent software industry monopolist, because of all the money they can make from you.

To quote whistleblower Ed Snowden, "I don't want to live in a world where everything that I say, everything I do, every thought, every aspiration, everyone I talk to, every expression of creativity or love or friendship is recorded and stored permanently.”

Remember, there is no cloud. That is just another corporate euphuism for other people’s computers (servers). In the cloud your personal information is not yours, but theirs.

They cannot be trusted, as they have a proven history of not being able to protect your data, and of using it in personally detrimental ways. You have everything to lose.

https://firewalltimes.com/recent-data-breaches/

The monopolist claim that data (your personal information) is like the new oil. They are leaking it everywhere.

Google Ordered Russian Translators Not to Call War in Ukraine a War

Internal email shows that despite its anti-war stance, the company bowed to Kremlin decrees.

https://theintercept.com/2022/03/28/google-russia-ukraine-war-censorship/

Google Issues Third Emergency Fix for Chrome This Year (theregister.com) 23

Posted by msmash on Friday April 15, 2022 @02:45PM from the security-woes dept.

Google is issuing fixes for two vulnerabilities in its Chrome web browser, including one flaw that is already being exploited in the wild. From a report: The emergency updates the company issued this week impact the almost 3 billion users of its Chrome browser as well as those using other Chromium-based browsers, such as Microsoft Edge, Brave and Vivaldi. It is the third such emergency update Google has had to issue for Chrome this year. One of the flaws is a type confusion vulnerability tracked as CVE-2022-1364, a high-severity, zero-day bug that is actively being used by attackers. With a type confusion flaw, a program will allocate a resource like a pointer or object using one type but later will access the resource using another, incompatible type. In some languages, like C and C++, the vulnerability can result in out-of-bounds memory access. This incompatibility can

cause a browser to crash or trigger logical errors. However, if exploited, it could enable a hacker to execute arbitrary code.

Documents Reveal Advanced AI Tools Google Is Selling to Israel

Google employees, who have been kept in the dark about the "Nimbus" AI project, have concerns about Israeli human rights abuses.

https://theintercept.com/2022/07/24/google-israel-artificial-intelligence-project-nimbus/

Stop Using Amazon

I know, I know, this is a hard one for me to write as well.

I have never purchased anything at a Walmart store, in part because they treat their employees badly; put two people out of work for everyone they hire, and love to suck off the government corporate welfare teat. They have put some of my favorite business out of business where I have lived. Wolahan's for good lumber, Thrifty Mac's for any hardware you can imagine, K-Mart for underwear.

Now it is the same for Amazon

Treat employees badly, and have a large carbon footprint.

Digital command, robots into action, persons picking, airplanes, trucks etc. just get something simple to me.

Reduced inventory at home improvement stores. It is frustrating to shop these days at grocery stores and home improvement stores.

I went to Lowe's looking for some gutter slash guards and they did not have any. Then I went to Menards and they had some, but only in white for my brown gutters. They had lots of brown gutter pipes and elbows but no brown screws. How many of these parts are they going to sell without brown screws? So what to do? Shop Amazon.com, and put my digital commands into their datacenters, putting robots into action, persons picking, airplanes loading, trucks delivering etc. just to get something simple to me. I could feel my carbon footprint expanding.

Simply things are no longer available in grocery stores either. Want some particular soap or shampoo you have been buying for years or decades. They do not have it. They have hundreds of different odd Generation X, Y, and Z brands, but not basic simple stuff.

It is like going to buy a potato and only being able to get a twice-baked, sour cream and onion with chives variety.

What to do? Shop Amazon.com, and put my digital commands into their datacenters, putting robots into action, persons picking, airplanes loading, trucks delivering etc.

Sure, you have to buy a case of soap or shampoo, but I still buy green bananas as well.

Amazon Datacenter

Ring Ukraine News Suppressed at Amazon's Request, Journalists Say

https://theintercept.com/2020/01/24/amazon-ring-ukraine/

I Want You Back: Getting My Personal Data From Amazon Was Weeks of Confusion and Tedium

I asked Amazon to provide the data it had collected on me. The process was a labyrinthine endurance test.

https://theintercept.com/2022/03/27/amazon-personal-data-request-dark-pattern/

This author's five novels are published on leanpub.com under the pseudonym Lefty Insider. He also publishes articles on medium.com under the same pseudonym.

"Freedom is something that dies unless it's used." Journalist Hunter S. Thompson

Literary Source References:

Schneier on Security
https://www.schneier.com/books/
A User's Guide to the Dark Web (and Clear Web)
(The 42nd and Final Encyclopedia Cyberspacia)
By Lefty Insider (arister0s n0stis)
https://leanpub.com/encyclopediacyberspacia

Postscript

It's getting worse out there people!

Experts Dissect Broadband Measurement Approaches as Federal Programs Roll Out

https://broadbandbreakfast.com/experts-dissect-broadband-measurement-approaches-as-federal-programs-roll-out/

"On the other hand, Darr presented data showing how speed testing technology has evolved, with many internet service providers now embedding testing capabilities directly in customer premises equipment."

So this new bandwidth (testing) data harvesting by rent-seeking monopoly incumbent ISP's, facilitated by Ookla CPE firmware, combined with their existing customer personal data harvesting (unless you are using a VPN) magically becomes a proprietary corporate asset for them to monetize.

At least with a Rewards card, you get a discount in exchange for them harvesting and monetizing your personal information. Here you get a big fat nothing from this theft. Sheesh!

This VPN Lets Anyone Use Your Internet Connection. What Could Go Wrong? (wired.com) 15

Posted by msmash on Friday December 20, 2024 @07:00AM from the closer-look dept.

Teenagers using Meta's virtual reality headsets to cheat at the popular game Gorilla Tag are unknowingly selling access to their home internet connections to potential cybercriminals, cybersecurity researchers found. The players have been side-loading Big Mama VPN, a free Android app, onto their VR headsets to create lag that makes it easier to win the tag-based game. However, the app simultaneously operates as a residential proxy service, selling access to users' IP addresses on a marketplace frequented by cybercriminals.

Cybersecurity firm Trend Micro discovered VR headsets were the third most common devices using Big Mama VPN, after Samsung and Xiaomi devices. The company's proxy services have been promoted on cybercrime forums and were linked to at least one cyberattack, according to research from security firms Trend Micro and Kela.

Feds Warn SMS Authentication Is Unsafe (gizmodo.com) 61

Posted by BeauHD on Thursday December 19, 2024 @04:33PM from the PSA dept.

An anonymous reader quotes a report from Gizmodo: *Hackers aligned with the Chinese government have infiltrated U.S. telecommunications infrastructure so deeply that it allowed the interception of unencrypted communications on a number of people, according to reports that first emerged in October. The operation, dubbed Salt Typhoon, apparently allowed hackers to listen to phone calls and nab text messages, and the penetration has been so extensive they haven't even been booted from the telecom networks yet. The Cybersecurity and Infrastructure Security Agency (CISA) issued guidance this week on best practices for protecting "highly targeted individuals," which includes a new warning (PDF) about text messages.*

"Do not use SMS as a second factor for authentication. SMS messages are not encrypted—a threat actor with access to a telecommunication provider's network who intercepts these messages can read them. SMS MFA is not phishing-resistant and is therefore not strong authentication for accounts of highly targeted individuals," the guidance, which has been posted online, reads. Not every service even allows for multi-factor authentication and sometimes text messages are the only option. But when you have a choice, it's better to use phishing-resistant methods like passkeys or authenticator apps. CISA prefaces its guidance by insisting it's only really speaking about high-value targets. The telecommunications hack mentioned above has been called the "worst hack in our nation's history," according to Sen. Mark Warner (D-VA).

This story was written by a human, not by Grammarly GO, ChatGPT, Jasper AI, GrowthBar, Frase, Copysmith, Hypotenuse, Copy AI, Writer, InferKit, Quillbot, Writesonic, Ryter, Gemini, or any other AI text generator.

This is the tenth in a series of articles on Broadband Internet

An Informed Citizens View of the Current Broadband CyberSecurity Kerfuffle (Part Six)

(Why can't we make the Internet a safe place for our children, and grandchildren to live and work?)

OpSec is the term used by computer security professionals as shorthand for operational security. Keeping the bad guys from getting at your computer, or other Internet connected devices to be able to extract or exfiltrate your personal information. There are many, many, layers to this idea.

This following republishes some writings regarding what the Internet could be.

Broadband Internet for All

As background to this piece, I have spent much of my adult life working to bridge the Digital Divide of access to computers and Internet service. I did this by refurbishing many thousands of corporate surplus computers for use by schools, nonprofits, and low-income families. And also by running a low cost dial in phone line Internet service to provide Internet access for many hundreds of families, and connect them to the Internet via a wireless broadband connection from a local ISP, and later with a DSL connection from a telecom provider.

First a bit of more relevant history.

History is clear in that without a massive public investment, there would be no Internet. It is also clear that we now need a broadband plan would take the first steps towards returning the Internet to its rightful owners, the public. This will ensure that everyone can have reliable, high-speed broadband.

Right now, nearly half of Americans do not have an Internet connection that meets minimum broadband speeds. Moreover, a staggering number of poor people of color do not have home Internet access of any kind. Yet Americans are charged some of the highest prices for Internet service in the developed world. These are all symptoms of a much larger, structural problem: the corporate capture of the pipes, wires, and other infrastructure that powers the Internet.

H.R.3152 - Rural Broadband Initiative Act 114th Congress (2015-2016)

To amend the Rural Electrification Act of 1936 to establish an Office of Rural Broadband Initiatives in the Department of Agriculture because the Rural Electrification Act of 1936 helped bring electricity and telephone service to rural America, thus removing major barriers to the development of our rural economies. A lack of affordable broadband presents a similar barrier to the development of our rural economy. According to the FCC, 53 percent of rural Americans lack access to service delivering broadband speeds of 25 Mbps for downloads and 3 Mbps for uploads. High-speed broadband access helps rural communities compete and grow in our digital economy. Died in Congress. Legislation not enacted in the current session of Congress is forever cleared from the books.

It Now Seems as if Another Internet Connection Method is Actually Possible

Over the past 20 years across the country, hundreds of cities and towns have taken it upon themselves to build their own publicly owned broadband networks. In general, these networks are cheaper, faster, and operate with greater public accountability, despite lacking their enormous economies of scale. Despite having been fought against tooth and nail by the incumbent ISP's.

https://muninetworks.org/

Current proposed High-Speed Internet for All plans provide Federal support for local broadband initiatives, or Internet cooperatives. The plans propose billions in infrastructure grants to be distributed to municipalities and states that want to voluntarily build out publicly owned and democratically controlled co-operative, open access broadband networks.

These plans do not build broadband infrastructure, but make the political terrain more tolerant of the expansion of public broadband initiatives. This is done by providing funding and technical assistance, and repealing laws in twenty-five states that prohibit or inhibit municipalities from building their own networks.

These public broadband networks would invest in low-income neighborhoods and would be required to abide by universal service requirements. These networks would be required to deploy technologies that meet minimum speed thresholds, and would condition grants on and adherence to strong labor, wage, and sourcing standards.

The funding sources for all of this new democracy are unclear at this point, but hey, how about we get some of that $400 billion back? Perhaps a tax or a rebate in exchange for no prison time for the fraud and extortion carried out against all of us.

Under these plans, the FCC would be de-neutered and be again able to regulate the rates that for-profit ISPs can charge their subscribers. ISPs would also be required to offer a low-cost Internet plan, which would be fully subsidized by the government for low-income households. Eligibility for subsidized Internet

access would be tied to eligibility for means-tested social programs like SNAP and Medicaid, effectively integrating Internet access into the welfare state. This would put more money back in the hands of low-income families, and help close America's cavernous digital divide. Internet for All would also provide a source of jobs to construct and maintain the network. Installing high-speed Internet could also potentially attract greater capital investment.

We could have a "public option" for Internet service that brings competing services to everyone regardless of his or her city, state, or zip code. After all, the Internet was invented from a massive public investment. It should now be returned to its rightful owners.

Source info:

https://www.jacobinmag.com/2019/12/broadband-Internet-bernie-sanders

"With the development of the Internet we are in the middle of the most transforming technological event since the capture of fire. I used to think that it was just the biggest thing since the Gutenberg printing press, but now I think you have to go back further." John Perry Barlow, American poet, essayist, cattle rancher, and cyber-libertarian political activist

Free the Internet

First, a bit of history. The first version of the Internet was born as a science project of the Advanced Research Projects Agency of the United States Department of Defense. ARPANET as it was known in the late 1960s, was developed primarily for military use, and was funded mainly by US Government National Science Foundation (NSF) grant monies. Senator Al Gore Jr. from Tennessee, was a visionary on this subject, and thus was instrumental in advocating for this funding. The ARPANET was fundamentally about linking static read-only scientific and academic materials together; to assist the DOD with advanced forward thinking research much of it being conducted at universities all around the country.

The second version of the Internet came around 1995 when this primarily scientific and academic network was opened to the public and the control and management of it turned over to a nonprofit organization called IETF. The Internet Engineering Task Force is an open standards international membership-based non-profit organization, which develops and promotes voluntary Internet standards. The Internet founders, including Tim Berners-Lee, also formed WW3, the World Wide Web Consortium as a standards body. It is interesting to note that Berners-Lee invented the web and then turned it over to the world.

As a reflection of humble beginnings, for the first 20 years domain registration was handled by one person, Jon Postel. Then they formed ICANN, The Internet Corporation for Assigned Names and Numbers. It is responsible for coordinating the maintenance and procedures the databases related to the namespaces and numerical spaces of the Internet, (called DNS) ensuring the network's stable and

secure operation. They also started charging for registering domain names. The Internet remained in a beta (developmental) stage, being originally developed and designed for sharing of information by people based on an idealistic honor system. This then further developed into a linked data semantic web with the development of a browser, funded with grant money by the NSF yet again.

When corporations started driving the WW3 is where things started to go wrong. This is when the original decentralization standard was murdered and corporations started to seize control and enact its perverted vision of Manifest Destiny over the data of citizens worldwide. The founders believed that the Internet/Web was about augmenting our collective intelligence as a species. A fight has been raging to overcome this evil ever since, despite the oversized egos of the builder hackers, and to bring decentralized identity verification for financial transactions and social media applications to the Web.

This pubic opening also led to the incubation of many startup companies driving ecommerce, the expansion of access to human knowledge, the proliferation of both digital music and cat video's, as well as tremendous economic and social growth. This second version was fundamentally about being interactive for read and write and for linking to programs which by the 2000's had evolved to include social media, and a large number of new businesses.

Those of us who enjoyed this phase during the 1990's now look back fondly at how joyful this experience was, even on a 56k or slower dialup connection, or 256k slow broadband connection. We now look back ashamedly at how single mindedly technically focused, and naïve we were about the dirty world around us.

Back in the 1990's no one had worried about all the disparate data being collected by the earlier computers, because we thought we knew there would never be a way to aggregate it all these disparate databases into anything useful to anyone. We were all wrong, very, very, horribly wrong.

The unregulated profit incentives birthed server farms, and Internet clouds, web crawlers, bots, and the algorithms to find, manipulate, and sort the big data of first a nation, and then the entire planet. These corporations have now built these dystopian parasitic surveillance machines, which prey on the entire human species.

Millions and then billions of simple minded and uninformed humans acted like oblivious lemmings all stepping off digital cliffs and into the corporate clouds. Their personal data is vacuumed like some giant digital spider spinning its web to entrap them and then sucking dry anything that smells like personal data from the transfer pipes containing the digital lives of billions of people on the planet.

Corporations profited from and used this data harvested through this predatory surveillance capitalism to alter the thinking, habits, purchases, and voting preferences of the masses in the now damaged and failing democracies. Yet these lemmings continued to carry these tracking devices with them and placed additional dystopian surveillance machine devices in their homes, on their homes, and in their cars, being misled by some misguided sense of convenience. They did this of course, because their connected parasitic devices told them to.

Those around the world now impoverished, unemployed and without hope from being on the wrong end of Western Empire building, became criminals to survive and who seek your money with phishing emails for malware and ransomware attacks on your computers.

Hacking is now persistent and accelerating in the number of ransomware, spyware, malware, and other computer intrusions and infections. This is due most of the entire world being able to access the Internet and those with bad intent able to scan the globe for individual computer weaknesses. It no longer matters if you are an individual, a small business, or a large one. You will be targeted if a weakness is spotted, regardless.

Of course, the American National Security Agency or NSA is hovering up all worldwide digital communications under the guise of Signals Intelligence (SISINT). Using their significant computer power to translate all of these zeros and ones into Human Intelligence (HUMINT) to know everything about everyone. "Collect it all," they said. They are storing all of this data on a server farm in Utah… forever.

So obviously based on the current rate of hacking of systems, resulting data breeches, and data collection, we know our software tools in use now are badly broken. People are being harmed, and some would go even further to say robbed, enslaved, and terrorized. I dread the day when some mad genius applies Artificial Intelligence (AI) to these hacking tools and fundamentally kills the Internet, as we know it. Perhaps we will all then need to hide out on the Dark Web, although the TOR browser has its own problems with metadata leakage and with NSA monitoring of the entry and exit nodes.

"Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one does not want the whole world to know, but a secret matter is something one does not want anybody to know. Privacy is the power to selectively reveal oneself to the world." Eric Hughes, 1993

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask those of you from the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather." — John Perry Barlow, "A Declaration of the Independence of Cyberspace" February, 1996

https://www.eff.org/cyberspace-independence

Yet the very insecure idealistic open architecture of the Internet web is what prevents privacy today, but every once in a while the good guys win one.

California Net Neutrality Law To Remain Intact After Appeals Court Says It Won't Reconsider Earlier Decision (theverge.com) 14

Posted by msmash on Thursday April 21, 2022 @04:08PM from the moving-forward dept.

A federal appeals court has denied a request for a rehearing on its January decision that upholds California's net neutrality law. From a report: The 2018 law, widely considered the strongest in the US, was signed into law a year after the Federal Communications Commission (FCC) repealed the Open Internet Order. That order had established stringent net neutrality rules that prohibited Internet service providers from throttling or blocking legal websites and apps, and banned ISPs from prioritizing paid content. California's law, which finally took effect last year, also prohibits throttling and speed lanes. Wireless trade associations including the NCTA, the CTIA, and ISPs including Comcast, Verizon, and AT&T sued to block California's law from taking effect, saying the FCC decision should preempt the state law. But that challenge was rejected by a district court judge.

The Ninth Circuit voted 3-0 in January to uphold the lower court ruling, saying the FCC "no longer has the authority" to regulate broadband Internet services because the agency reclassified them as "information services, instead of telecommunications services. The FCC therefore cannot preempt the state action." FCC chairwoman Jessica Rosenworcel praised the decision on Twitter, reiterating her position that she wants to see net neutrality become "the law on the land" again. The FCC can't currently reinstate net neutrality at the federal level however since the panel lacks a majority and the two Democrats and two Republicans remain deadlocked on the issue. President Biden's FCC nominee Gigi Sohn is still awaiting a confirmation vote in the Senate.

A Clear and Transparent Digital Bill of Rights

1. A customer must consent or opt in when personal information is collected or shared with a third party and must be able to limit the use of information not required to provide the requested service
2. A customer must be able to obtain, edit, and delete personal information held by a vendor
3. A customer must be notified immediately when the security of this information is breeched
4. A customer must be able to move his/her collected information in a conveniently useable and machine-readable format

What is considered personal data under the EU GDPR?

The European Union's General Data Protection Regulation (GDPR) tries to strike a balance between being strong enough to give individuals clear and tangible protection while being flexible enough to allow for the legitimate interests of businesses and the public. As part of this balancing act, the GDPR goes to great lengths to define what is and is not personal data.

https://gdpr.eu/eu-gdpr-personal-data/

EU agrees rules to force big tech to rein in illegal content or face huge fines

Digital Services Act can now fine platforms like Facebook, Google and Twitter up to 6% of their global revenue

Large online platforms including Facebook, Google and Twitter will have to do more to tackle illegal content or face multibillion euro fines under a new European Union regulatory regime agreed on Saturday.

The wide-ranging Digital Services Act (DSA) can fine a company up to 6% of its global turnover for violating the rules – which would be $7bn (£5.9bn) in the case of Facebook's owner – while repeated breaches could result in a tech firm being banned from doing business in the EU.

https://www.theguardian.com/world/2022/apr/23/eu-agrees-rules-to-force-big-tech-to-rein-in-content-or-face-huge-fines

I hope that now by the end of these articles, you are a lot more knowledgeable and capable of keeping:

In the words of Julian Assange, *"Keep Calm and Encrypt."*

Contract-for-the-Web

Contract for the Web-Principles

PRINCIPLE 1

Governments will Ensure everyone can connect to the Internet So that anyone, no

matter who they are or where they live, can participate actively online

PRINCIPLE 2

Keep all of the Internet available, all of the time so that no one is denied their right to full Internet access

PRINCIPLE 3

Respect and protect people's fundamental online privacy and data rights so everyone can use the Web freely, safely and without fear

PRINCIPLE 4

Make the Internet affordable and accessible to everyone so that no one is excluded from using and shaping the web

PRINCIPLE 5

Respect and protect people's privacy, personal data, and other online data rights to build online trust so people are in control of their lives online, empowered with clear and meaningful choices around their data and privacy

PRINCIPLE 6

Companies will develop technologies that support the best in humanity and challenge the worst so the web really is a public good that puts people first

PRINCIPLE 7

Citizens will be creators and collaborators on the web so the web has rich and relevant content for everyone

PRINCIPLE 8

Citizens will build strong communities that respect civil discourse and human dignity so that everyone feels safe and welcome online

PRINCIPLE 9

Citizens will fight for the web so the web remains open and a global public resource for people everywhere, now and in the future

Download the PDF https://contractfortheweb.org/

Declaration-for-the-Future-for-the-Internet

The White House issued a 'Declaration for the Future of the Internet ' on April 28, 2022, in partnership with 60 other nations and global accords, which outlined the United States' agenda for the Internet under President Joe Biden.

We are united by a belief in the potential of digital technologies to promote connectivity, democracy, peace, the rule of law, sustainable development, and the enjoyment of human rights and fundamental freedoms. As we increasingly work,

communicate, connect, engage, learn, and enjoy leisure time using digital technologies, our reliance on an open, free, global, interoperable, reliable, and secure Internet will continue to grow. Yet we are also aware of the risks inherent in that reliance and the challenges we face.

We call for a new Declaration for the Future of the Internet that includes all partners who actively support a future for the Internet that is an open, free, global, interoperable, reliable, and secure. We further affirm our commitment to protecting and respecting human rights online and across the digital ecosystem. Partners in this Declaration intend to work toward an environment that reinforces our democratic systems and promotes active participation of every citizen in democratic processes, secures and protects individuals' privacy, maintains secure and reliable connectivity, resists efforts to splinter the global Internet, and promotes a free and competitive global economy. Partners in this Declaration invite other partners who share this vision to join us in working together, with civil society and other stakeholders, to affirm guiding principles for our role in the future of the global Internet.

Reclaiming the Promise of the Internet

The immense promise that accompanied the development of the Internet stemmed from its design: it is an open "network of networks," a single interconnected communications system for all of humanity. The stable and secure operation of the Internet's unique identifier systems have, from the beginning, been governed by a multi-stakeholder approach to avoid Internet fragmentation, which continues to be an essential part of our vision. For business, entrepreneurs, and the innovation ecosystem as a whole, interconnection promises better access to customers and fairer competition; for artists and creators, new audiences; for everyone, unfettered access to knowledge. With the creation of the Internet came a swell in innovation, vibrant communication, increased cross-border data flows, and market growth—as well as the invention of new digital products and services that now permeate every aspect of our daily lives.

Over the last two decades, however, we have witnessed serious challenges to this vision emerge. Access to the open Internet is limited by some authoritarian governments and online platforms and digital tools are increasingly used to repress freedom of expression and deny other human rights and fundamental freedoms. State-sponsored or condoned malicious behavior is on the rise, including the spread of disinformation and cybercrimes such as ransomware, affecting the security and the resilience of critical infrastructure while holding at risk vital public and private assets. At the same time, countries have erected firewalls and taken other technical measures, such as Internet shutdowns, to restrict access to journalism, information, and services, in ways that are contrary to international human rights commitments and obligations. Concerted or independent actions of some governments and private actors have sought to abuse the openness of Internet governance and related processes to advance a closed vision. Moreover, the once decentralized Internet economy has become highly concentrated and many people have legitimate concerns about their

privacy and the quantity and security of personal data collected and stored online. Online platforms have enabled an increase in the spread of illegal or harmful content that can threaten the safety of individuals and contribute to radicalization and violence. Disinformation and foreign malign activity is used to sow division and conflict between individuals or groups in society, undermining respect for and protection of human rights and democratic institutions.

Our Vision

We believe we should meet these challenges by working towards a shared vision for the future of the Internet that recommits governments and relevant authorities to defending human rights and fostering equitable economic prosperity. We intend to ensure that the use of digital technologies reinforces, not weakens, democracy and respect for human rights; offers opportunities for innovation in the digital ecosystem, including businesses large and small; and, maintains connections between our societies. We intend to work together to protect and fortify the multi-stakeholder system of Internet governance and to maintain a high level of security, privacy protection, stability and resilience of the technical infrastructure of the Internet.

We affirm our commitment to promote and sustain an Internet that: is an open, free, global, interoperable, reliable, and secure and to ensure that the Internet reinforces democratic principles and human rights and fundamental freedoms; offers opportunities for collaborative research and commerce; is developed, governed, and deployed in an inclusive way so that unserved and underserved communities, particularly those coming online for the first time, can navigate it safely and with personal data privacy and protections in place; and is governed by multi-stakeholder processes. In short, an Internet that can deliver on the promise of connecting humankind and helping societies and democracies to thrive.

The Internet should operate as a single, decentralized network of networks – with global reach and governed through the multi-stakeholder approach, whereby governments and relevant authorities collaborate with academics, civil society, the private sector, technical community and others. Digital technologies reliant on the Internet, will yield the greatest dividends when they operate as an open, free, global, interoperable, reliable, and secure systems. Digital technologies should be produced, used, and governed in ways that enable trustworthy, free, and fair commerce; avoid unfair discrimination between, and ensure effective choice for, individual users; foster fair competition and encourage innovation; promote and protect human rights; and, foster societies where human rights and fundamental freedoms, and the well-being of all individuals are protected and promoted;

All can connect to the Internet, no matter where they are located, including through increased access, affordability, and digital skills; individuals and businesses can trust the safety and the confidentiality of the digital technologies they use and that their privacy is protected;

• Businesses of all sizes can innovate, compete, and thrive on their merits in a fair and competitive ecosystem;

- Infrastructure is designed to be secure, interoperable, reliable, and sustainable;
- Technology is used to promote pluralism and freedom of expression, sustainability, inclusive economic growth, and the fight against global climate change.

Principles to promote this Vision

The partners in this Declaration intend to uphold a range of key principles, set out below, regarding the Internet and digital technologies; to promote these principles within existing multilateral and multi-stakeholder fora; to translate these principles into concrete policies and actions; and, work together to promote this vision globally, while respecting each other's regulatory autonomy within our own jurisdictions and in accordance with our respective domestic laws and international legal obligations.

These principles are not legally binding but should rather be used as a reference for public policy makers, as well as citizens, businesses, and civil society organizations.

Protection of Human Rights and Fundamental Freedoms

Dedicate ourselves, in conducting and executing our respective domestic authorities, to respect human rights, including as reflected in the Universal Declaration of Human Rights, as well as the principles of the rule of law, legitimate purpose, non-arbitrariness, effective oversight, and transparency, both online and offline, and call upon others to do the same.

Promote online safety and continue to strengthen our work to combat violence online, including sexual and gender-based violence as well as child sexual exploitation, to make the Internet a safe and secure place for everyone, particularly women, children, and young people.

Promote safe and equitable use of the Internet for everyone, without discrimination based on sex, race, color, ethnic, national, or social origin, genetic features, language, religion, or belief, political or any other opinion, membership of an indigenous population, property, birth, disability, age, gender identity, or sexual orientation.

Reaffirm our commitment that actions taken by governments, authorities, and digital services including online platforms to reduce illegal and harmful content and activities online be consistent with international human rights law, including the right to freedom of expression while encouraging diversity of opinion, and pluralism without fear of censorship, harassment, or intimidation.

Protect and respect human rights and fundamental freedoms across the digital ecosystem, while providing access to meaningful remedies for human rights violations and abuses, consistent with international human rights law.

Refrain from misusing or abusing the Internet or algorithmic tools or techniques for unlawful surveillance, oppression, and repression that do not align with international human rights principles, including developing social score cards or other mechanisms of domestic social control or pre-crime detention and arrest.

A Global Internet

Refrain from government-imposed Internet shutdowns or degrading domestic Internet access, either entirely or partially.

Refrain from blocking or degrading access to lawful content, services, and applications

on the Internet, consistent with principles of Net Neutrality subject to applicable law, including international human rights law.

Promote our work to realize the benefits of data free flows with trust based on our shared values as like-minded, democratic, open, and outward looking partners.

Promote cooperation in research and innovation and standard setting, encourage information sharing regarding security threats through relevant international fora, and reaffirm our commitment to the framework of responsible state behavior in cyberspace.

Inclusive and Affordable Access to the Internet

Promote affordable, inclusive, and reliable access to the Internet for individuals and businesses where they need it and support efforts to close digital divides around the world to ensure all people of the world are able to benefit from the digital transformation.

Support digital literacy, skills acquisition, and development so that individuals can overcome the digital divide, participate in the Internet safely, and realize the economic and social potential of the digital economy.

Foster greater exposure to diverse cultural and multilingual content, information, and news online. Exposure to diverse content online should contribute to pluralistic public discourse, foster greater social and digital inclusion within society, bolster resilience to disinformation and misinformation, and increase participation in democratic processes.

Trust in the Digital Ecosystem

Work together to combat cybercrime, including cyber-enabled crime, and deter malicious cyber activity.

Ensure that government and relevant authorities' access to personal data is based in law and conducted in accordance with international human rights law.

Protect individuals' privacy, their personal data, the confidentiality of electronic communications and information on end-users' electronic devices, consistent with the protection of public safety and applicable domestic and international law.

Promote the protection of consumers, especially vulnerable consumers, from online scams, unfair practices online and from dangerous and unsafe products sold online.

Promote and use trustworthy network infrastructure/services suppliers, relying on risk-based assessments that include technical and non-technical factors for network security.

Refrain from using the Internet to undermine the electoral infrastructure, elections and political processes, including through covert information manipulation campaigns.

• Support a rules-based global digital economy, which fosters trade and contestable and fair online markets so that firms and entrepreneurs can compete on their merits.

• Cooperate to maximize the enabling effects of technology for combatting climate change and protecting the environment whilst reducing as much as possible the environmental footprint of the Internet and digital technologies.

Multi-stakeholder Internet Governance

Protect and strengthen the multi-stakeholder system of Internet governance, including the development, deployment, and management of its main technical protocols and other related standards and protocols.

Refrain from undermining the technical infrastructure essential to the general availability and integrity of the Internet.

We believe that the principles for the future of the Internet are universal in nature and

as such we invite those who share this vision to affirm these principles and join us in the implementation of this vision. This Declaration takes into account, and expects to contribute to, existing processes in the UN system, G7, G20, the Organization for Economic Cooperation and Development, the World Trade Organization, and other relevant multilateral and multi-stakeholder fora, the Internet Corporation for Assigned Names and Numbers, Internet Governance Forum, and Freedom Online Coalition. We also welcome partnership with the many civil society organizations essential to promoting an open, free, global, interoperable, reliable, and secure Internet, and defending fundamental freedoms and human rights online. Partners in this Declaration intend to consult and work closely with stakeholders in carrying forward this vision. April 2022 ★ ★ ★ ★ ★

"There are two types of companies: those that have been hacked, and those who don't know they have been hacked." — John Chambers, CEO Cisco

Postscript

It's getting worse out there people!

How to Lose a Fortune with Just One Bad Click (or why not to get involved with Google)
https://krebsonsecurity.com/2024/12/how-to-lose-a-fortune-with-just-one-bad-click/

Literary Source References:

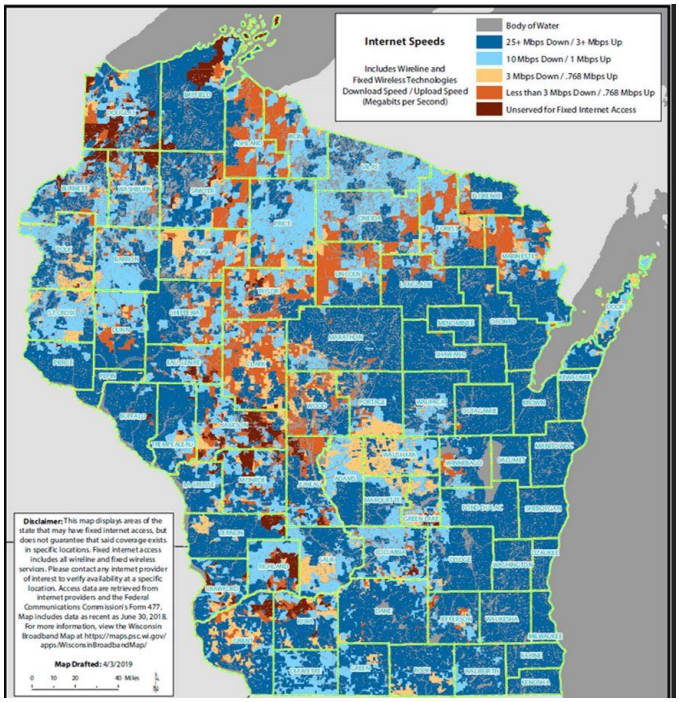
Schneier on Security
https://www.schneier.com/books/
A User's Guide To The Dark Web (and Clear Web)
(The 42nd and Final Encyclopedia Cyberspacia)
By Lefty Insider (arister0s n0stis)
https://leanpub.com/encyclopediacyberspacia

This story was written by a human, not by Grammarly GO, ChatGPT, Jasper AI, GrowthBar, Frase, Copysmith, Hypotenuse, Copy AI, Writer, InferKit, Quillbot, Writesonic, Ryter, Gemini, or any other AI text generator.

Note: This is the thirteenth in a series of articles on Broadband Internet

An Informed Citizens View of the Current Wisconsin Broadband Kerfuffle (Extended)

(We all need to fully understand this problem to be able to solve it)


Internet Speeds
Includes Wireline and Fixed Wireless Technologies Download Speed / Upload Speed (Megabits per Second)
Body of Water
25+ Mbps Down / 3+ Mbps Up
10 Mbps Down / 1 Mbps Up
3 Mbps Down / .768 Mbps Up
Less than 3 Mbps Down / .768 Mbps Up
Unserved for Fixed Internet Access
Disclaimer: This map displays areas of the state that may have fixed internet access, but does not guarantee that said coverage exists in specific locations. Fixed internet access includes all wireline and fixed wireless services. Please contact any internet provider of interest to verify availability at a specific location. Access data are retrieved from internet providers and the Federal Communications Commission's Form 477. Map includes data as recent as June 30, 2018. For more information, view the Wisconsin Broadband Map at https://maps.psc.wi.gov/apps/WisconsinBroadbandMap/
Map Drafted: 4/3/2019

Internet speeds across the state

Wisconsin's broadband infrastructure also consistently ranks near the bottom of states in the nation. *"Wisconsin currently ranks 38th for Internet access, out of all 50 states."* Wisconsin Public Radio, February 12, 2020.

More recently in December, 2024 the state rating dropped 10 points to 48th, neighboring Minnesota has seen a 38% increase to improve to 34th on the list. Neighboring Michigan is 39th on the list

47	Maine	42.5
48	Wisconsin	42.2
49	Wyoming	39.0
50	Alaska	38.0
51	Montana	31.5

State Ranking and Percentage of Speedtest users achieving broadband speeds of 100/20 Mbps
https://www.ookla.com/research/market-reports/h1-2024-50-u-s-states-broadband-speed-performance?submissionGuid=5888725b-1ed5-4e0b-a391-e31d14b48423

21	Mississippi	56.5
22	Georgia	55.7
23	Alabama	55.6

Wisconsinites not shocked and ashamed yet? How about the above comparison data?

This situation is not something that is unknown to our government agencies and legislative representatives.

DATCP State Consumer Complaints

Telecommunications Complaints (642)

The Dept. of Agriculture, Trade and Consumer Protection or DATCP, received 642 complaints regarding telecommunications services in 2023, down slightly from the previous year. Consumers reported issues including billing disputes, disconnections, and terminations of service, deceptive and misleading representations, refund and adjustment policies, and failure to cancel services when requested. Consumers should carefully read their contracts and policies to understand the extent and limitations of the services they are purchasing.

https://datcp.wi.gov/Pages/News_Media/20240201TopTenConsumerComplaintsReportedtoDATCPin2023.aspx

Dept. of Agriculture, Trade and Consumer Protection: Aids Wisconsin consumers:

Top ten consumer complaints in 2021

Telecommunications Complaints (573)

Disputes with telecommunications companies continued to be a concern for many Wisconsinites, but overall the category dropped two places in the ranking. Consumers reported issues such as billing disputes, misleading advertisements, and termination of services as principal concerns.

https://www.wispolitics.com/2022/dept-of-agriculture-trade-and-consumer-protection-aids-wisconsin-consumers-top-ten-consumer-complaints-in-2021/

So 2000 or so telecommunication complaints (top 4 or 10) that the DATCP has already collected over the past few years. I would suggest, without direct knowledge, that a good percentage of these represent Internet speed complaints.

https://datcp.wi.gov/Pages/News_Media/20240201TopTenConsumerComplaintsReportedtoDATCPin2023.aspx

Wisconsinite State DATCP complaints

https://datcp.wi.gov/Pages/Programs_Services/Complaints.aspx

And these are only those who actually have access, and are among the few who actually will make a written complaint.

"The Loyalty Effect" by Frederick Reichheld: Reichheld, a well-known figure in customer loyalty research, highlights that most unhappy customers do not complain; they simply leave. He estimates that the typical company only hears from 4-5% of dissatisfied customers.

"Customer Experience 3.0" by John A. Goodman: Goodman's research and writings on customer experience and service recovery emphasize that although complaints are vital for understanding customer dissatisfaction, only a small percentage of unhappy customers will actually lodge formal complaints. In fact, Goodman points out that for every customer who complains, there are likely 26 others who are dissatisfied but don't speak up.

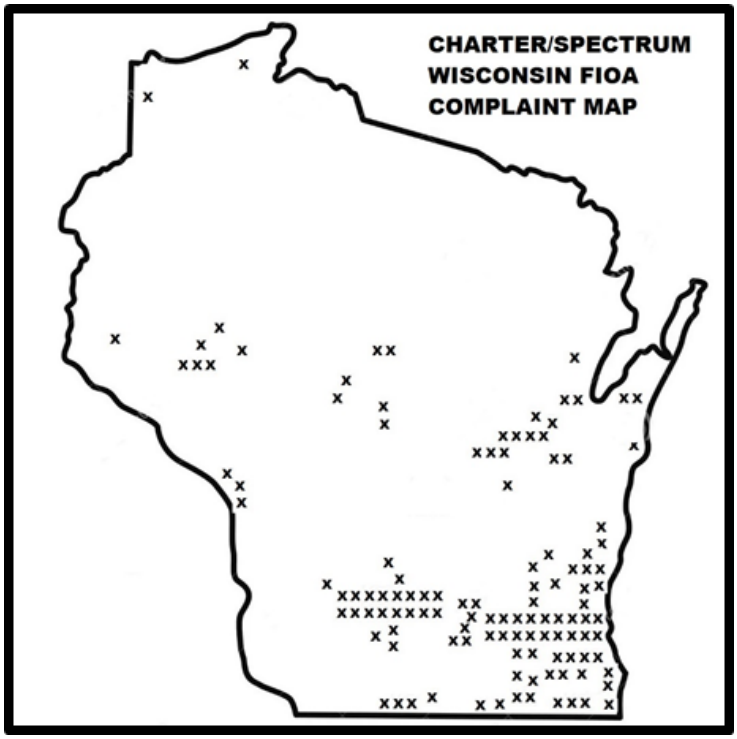
Federal Consumer Complaints

Wisconsinite Federal FCC complaints can be made here:
https://consumercomplaints.fcc.gov/hc/en-us
Internet specific complaints can be made here:
https://consumercomplaints.fcc.gov/hc/en-us/articles/115002206106-Internet-Form-Descriptions-of-Complaint-Issues

My own personal FCC complaints:
April 8/June 2, 2021 FCC Ticket #4692199, April 10, 2021 FCC Ticket #4703882, April 24, 2021 FCC Ticket #4735423, May 4/17, 2021 FCC Ticket #4682719, April 10/May 16, 2023 FCC Ticket #6123084, May 8, 2023 FCC Ticket #6263554, November 23, 2024 FCC Ticket Number 7378474, December 23,2024 FCC Ticket # 7542363, December 29, Ticket No. 7550355 and Ticket No. 7550359, December 30, 2024 Ticket No. 7552213 (comparing the dates and ticket numbers you can see lots of claims)
Freedom of Information Act or FOIA, requests can be make here:
https://www.foia.gov/agency-search.html?id=ee57c611-328a-4178-9f1c-441fe0f93141&type=component

Choice is quite impossible when you have none.

"But let me be very clear: Capitalism without competition isn't capitalism; it's exploitation. Without healthy competition, big players can change and charge whatever they want and treat you however they want." Remarks by President Biden At Signing of An Executive Order Promoting Competition in the American Economy July 09, 2021



The above map was created from data in a Freedom of Information Act or FOIA request made to the Federal Communications Commission or FCC.

These complaints were from most all areas of the state that actually have Charter wireline Internet connections. (This graphic shows complaints about Charter Communications/Spectrum only). This graphic does not include complaints from Comcast, Frontier, TDS or other wireline ISP's.

There were **123** Charter speed complaints filed from 2018-2024. They make for interesting, disturbing, and infuriating reading. Monopolistic, malevolent, lawless, and evil behaviors are laid bare for anyone to see. (These complaints will be articulated in full in a future novel published on leanpub.com (The Insider Goes Deep into Consumer Protection) and are also currently available online at www.tcw.org/FCC FOIA request documents.pdf

This one particular complaint example below is ***exactly*** indicative of my own personal experience.

Ticket: # 7023912 - Spectrum is engaging in misleading and predatory business
Date: 5/10/2024 11:52 PM
City/State/Zip: Madison, Wisconsin 53718-3041
Company Complaining About: Spectrum

Description

Recently I upgraded my Internet with Spectrum to gigabit. However, since the upgrade my Internet speeds had significantly reduced compared to previously and was unable to reach 400mbps despite advertised as gigabit. Customer service was unable to resolve the issue, so I requested my account be reverted back to the previous plan. Now my bill has increased due to removal of a promotional offer that was not set to expire until 2026. I am being punished for not accepting an upgrade that could not even deliver at 50% of the advertised speed.

Note: Please keep in mind that it is only a percentage of the aggrieved and exploited who will actually file a complaint. And even less actually know about the DATCP complaint process.

What percentage of customers will file a written complaint about a service?

CHATGPT says: The percentage of customers who file a written complaint about a service tends to be relatively low. Research suggests that only about 1-5% of dissatisfied customers will actually take the time to file a formal complaint, either in writing or through official channels.The exact number can vary depending on the industry, the nature of the service, and the company's customer service practices. Most dissatisfied customers will simply stop using the service, or express their dissatisfaction in less formal ways, such as through word-of-mouth or online reviews.

Several factors influence the likelihood of a written complaint, such as:

- **Severity of the problem**: More serious issues tend to result in formal complaints.
- **Customer engagement**: Customers who feel invested in the service or have a high level of loyalty might be more inclined to file a complaint.
- **Ease of the complaint process**: If it's easy to file a complaint or contact customer service, more customers might take that step.
- **Customer expectations**: Customers with higher expectations are more likely to complain when those expectations aren't met.

It is also worth noting that many customers who have a poor experience might choose not to escalate their complaint formally because they don't expect a resolution or don't feel that their voice will make a difference.

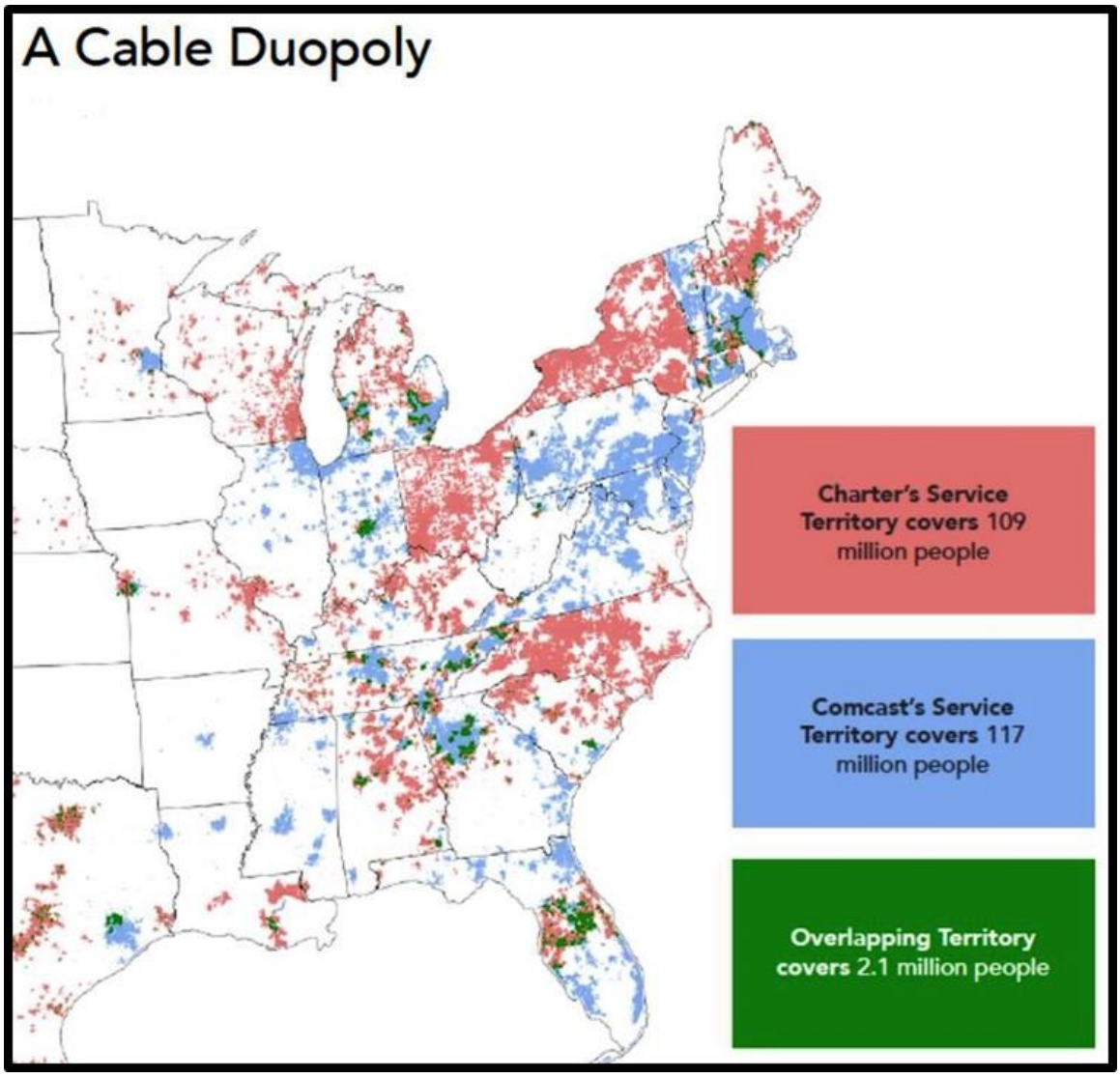
In doing some localized Internet speed testing I have discovered something disturbing to me.

The Charter/Spectrum technicians in this area are leaving the customer routers open, default admin, and admin UN and Password.

So that I or anyone could do anything with it, like shut it off, change the passwords, hack other connected users, inject a virus, use it as a bot to take down other systems, etc.

Again, this is Charter/Spectrum's own CPE that is installed here. (modem and router)

THIS IS A POTENTIAL NATIONAL SECURITY ISSUE!


A Cable Duopoly
Charter's Service Territory covers 109 million people
Comcast's Service Territory covers 117 million people
Overlapping Territory covers 2.1 million people

Choices? What choices?

The Potential (And Perhaps Short-Sited) Solutions

The Wisconsin Governor's broadband plan has everyone with a 100/20 Mbps minimum Internet connection by 2030 using government subsidy funding including:

The Broadband Equity, Access and Deployment or BEAD – some consider this program to be the cleanup hitter to follow what the other Federal broadband subsidy programs (RDOF, ARPA, etc.) have done. BEAD is about building supply infrastructure and the second punch is the Federal Digital Equity Act or DEA, which is about sustainable demand (affordability, accessibility, device and software skills, and technical support) Providing broadband access throughout Wisconsin communities often solves only half of a state's digital divide problem. Leveraging the power of the new connectivity in their daily lives is not something everyone knows how to do, and so digital literacy training is also needed.

There are 2,300,000 Locations Broadband Service Locations or (BSLs) in Wisconsin (business or residential location at which mass-market fixed broadband Internet access service is, or can be, installed)

Background: The Bipartisan Infrastructure Law allocated $42.5 Billion under the Broadband, Equity, Access, and Deployment (BEAD) Program for broadband infrastructure deployment. Wisconsin was awarded: $1,055,823,574.

1,900,000 Served or Ineligible (based on outdated and incorrect speed test data and maps)
425,000 unserved and underserved locations
206,715 Locations eligible for BEAD
200,000 In-Progress

Definition of "Underserved" under BEAD

The National Telecommunications and Information Administration (NTIA), which oversees the BEAD program, defines underserved as follows:

Speeds Below 100/20 Mbps, and where broadband is available, but the speeds and/or quality are not sufficient for modern needs.

- This threshold is a key metric used to determine areas that are underserved by current broadband providers.

Cost of Service:

- In some cases, a community may also be classified as underserved if broadband service is available but the cost of the service is prohibitively high or not affordable for a large portion of the population.
- If Internet access is available but unaffordable, the area might be eligible for BEAD funding to improve affordability and provide more equitable access.

No Wired Broadband Available:

- A location where no wired broadband (such as fiber, cable, or DSL) service is available could also be considered underserved, even if there are mobile or satellite options. The emphasis is on quality and reliability, and areas relying only on satellite or wireless solutions may qualify for BEAD funding. Underserved means speeds below 100/20 Mbps

Definition of "Unserved" under BEAD

The National Telecommunications and Information Administration (NTIA), which oversees the BEAD program, defines unserved as follows:

Unserved refers to areas that do not have any broadband access at all, meaning no Internet service meeting the 100/20 Mbps threshold is available.

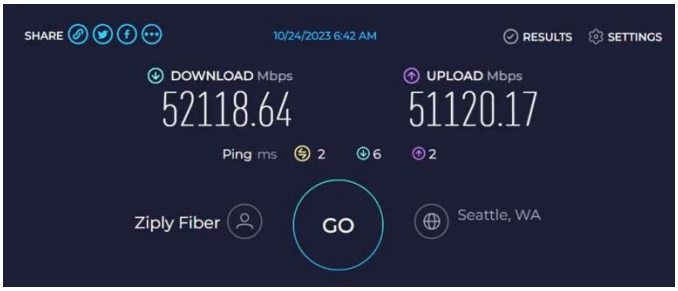
Construction of BEAD projects late 2025 to late 2029

In 2024, the Task Force continued to emphasize its goals established in the 2023 report, which are that:

• By 2028/2029, all homes and businesses will have access to high-speed broadband service that reliably provides a download speed of at least 100 Mbps and an upload speed of at least 20 Mbps.

Below is likely where Europe and Asia will be by then:

TO



The Current Impacts

Wisconsin Rural Broadband Efforts Largely Unnoticeable

In its first two years, the program has benefited just a few thousand households served by 14 Wisconsin service providers. Efforts to bridge rural broadband disparities fall well short of a solution for most outside of urban areas, according to Internet service providers and industry experts.

https://www.govtech.com/network/Wisconsin-Rural-Broadband-Efforts-Largely-Unnoticeable-.html

Despite billions of public dollars, some rural residents slog through slow Internet

A spokesperson for Madison-based TDS Telecom said it is difficult to say whether TDS would have expanded broadband service to rural areas without federal dollars.

https://madison.com/wsj/business/despite-billions-of-public-dollars-some-rural-residents-slog-through/article_a6d5f951-7937-5e37-b7dc-54b5fd88460c.html

TDS Telecom for example is currently in the process of providing upgraded fiber backbone to Wisconsin via the current Federal Rural Broadband Initiative. The plan covers the Madison and Wausau suburbs mostly in the central and western parts of the state, the least rural areas. This leaves the northeastern area out of luck, and gives our rural communities the choice of spotty cable service, slow expensive cellular service, or slow and even more expensive satellite service. https://tdsfiber.com/build/

Sorry zip code 54214, no fiber for you! Except for the "fiber to the telecom press releases," we continue to see over and over for many decades now.

For many years, Broadband Internet supporters have attempted to reconcile the public interest in universal, high-quality broadband against the profit motives of Internet Service Providers (ISPs). They tried to tame their malfeasance, but not break them up and leave their ownership and control of the Internet infrastructure intact.

It has now become clear that they are in fact responsible for the sorry state of broadband in this country, having received $400 Billion in subsidies and discounts over the past century that they have not lived up to. We should now make them pay us back to fix it. The Book of Broken Promises http://teletruth.org/

See also: America's Broadband Heroes: Fixed Wireless Broadband Providers www.wispa.org.

It is now well past the time to develop a vision of what a more democratic communication system that operates outside of the existing market would look like.

Some current presidential candidates have unveiled plans to create publicly owned broadband Internet networks as an expansion of, and eventual replacement for, the existing system. These plans create public interest regulations on existing ISP's, using antitrust legislation much as we currently regulate the companies that manage electricity, gas, and other critical infrastructure utilities in the United States. Most importantly, the plans would create publicly owned competitive alternatives to corporate ISPs.

So in the end, Rural Broadband service equals economic growth, by keeping Wisconsin's talented young people from leaving the rural areas of the state and not limiting their ability to thrive in a digital economy. As of 2017, US ranks 9th in the world in fixed broadband speed at 70.75 Mbps average, but this is less than half top-ranked Singapore's 154.38 Mbps. The US is also one of the most expensive nations: in 120th place (out of 195).with an average monthly cost of $67.69. Locally, Wisconsin ranks 41st in the United States in its ranking for Internet access, 32nd for broadband access with an average speed of 37.4 Mbps and coverage of 85.3%.

"In July 2013, the state created the Broadband Expansion Grant program to help meet the demand for improved broadband and encourage its development in Wisconsin's unserved and underserved areas. Since then, the PSC has awarded approximately $20.1 million to 138 grant projects over six years. In September 2019, the PSC opened the Broadband Expansion Grant applications for 2020. This grant cycle provides up to $24 million for improving Internet access across Wisconsin."

https://psc.wi.gov/Pages/Programs/WBO.aspx

This appears to be just enough money to say you did something…but not really.

Broadband access as a human right

Tang emphasized that in Taiwan, broadband access is a human right. *"If you do not have bidirectional (otherwise called symmetrical) access, then you're back to a broadcasting model where the download bandwidth is far higher than the uplink bandwidth,"* she said. *In some places in the world, it costs virtually nothing to download content, but it's far more expensive to live-stream and upload content.* For Tang, *"that asymmetry means that you do not have the right to participate." In a democracy in the digital age, bidirectional communication is foundational.* Audrey Tang of Taiwan's Sunflower Movement

Literary Source References:

"The Loyalty Effect" by Frederick Reichheld: Reichheld, a well-known figure in customer loyalty research, highlights that most unhappy customers do not complain; they simply leave. He estimates that the typical company only hears from 4-5% of dissatisfied customers.

"Customer Experience 3.0" by John A. Goodman: Goodman's research and writings on customer experience and service recovery emphasize that although complaints are vital for understanding customer dissatisfaction, only a small percentage of unhappy customers will actually lodge formal complaints. In fact, Goodman points out that for every customer who complains, there are likely 26 others who are dissatisfied but don't speak up.

Top Ten Consumer Complaints Reported to DATCP in 2023
https://datcp.wi.gov/Pages/News_Media/20240201TopTenConsumerComplaintsReportedtoDATCPin2023.aspx

AG Kaul, Secretary Romanski Secure $15 Million Agreement with Frontier Communications
https://datcp.wi.gov/Pages/News_Media/20220728DATCP-DOJFrontierCommunications.aspx

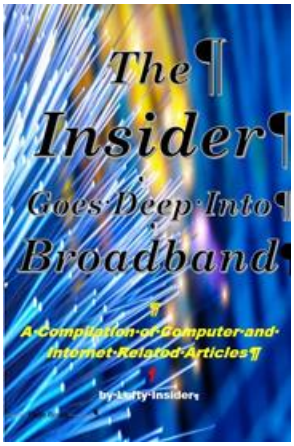
Top Ten Consumer Complaints Reported to DATCP in 2023
https://datcp.wi.gov/Pages/News_Media/20240201TopTenConsumerComplaintsReportedtoDATCPin2023.aspx

Task Force on Broadband Access 2023 report
By 2028/2029, all homes and businesses will have access to high-speed broadband service that reliably provides a download speed of at least 100 Mbps and an upload speed of at least 20 Mbps.
https://psc.wi.gov/Documents/broadband/2024GovernorsTaskForceOnBroadbandAccessReport.pdf

Wisconsin Allocates $115 Million in Broadband Funding for Anchor Institutions
https://broadbandbreakfast.com/wisconsin-allocates-115-million-in-broadband-funding-for-anchor-institutions/

Wisconsin GOP Cuts $750 Million from State Broadband Budget
https://broadbandbreakfast.com/wisconsin-gop-cuts-750-million-from-state-broadband-budget/

A full version of this article, and many others, are available for purchase at leanpub.com in novel format as The Insider Goes Deep into Broadband (A Compilation of Computer and Internet Related Articles).



The authors additional novels are also published on leanpub.com as well as many additional articles on medium.com under the pseudonym Lefty Insider

ChatGPT 4.0 was used as a research assistant, and no unedited AI generated text was used in this article.

Appendices

Appendix One - Bandwidth Error Messages **11**

Appendix Two - Speed Tests **12**

Appendix Three - VPN's **16**

Appendix Four - Beyond Speed Test Sites (FTP and QoE) **18**

Appendix Five Bandwidth Labels **20**

Appendix Six A Fiber Tale of Two Properties **22**

Appendix Seven VPN's (continued) **24**

Appendix Eight - FTP/SFTP - File Transfers **26**

Appendix Nine - Wisconsin Statute Annotated § 66.0422 **28**

Appendix Ten – DATCP **30**

Appendix Eleven – FCC **32**

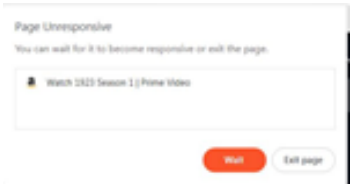
Appendix Twelve - What are some Solutions? **33**

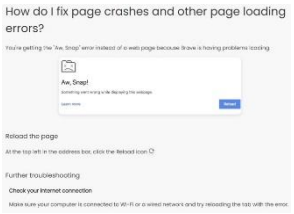
Appendix Thirteen – Conclusions **36**

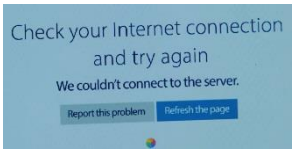
Appendix One Bandwidth Error Messages

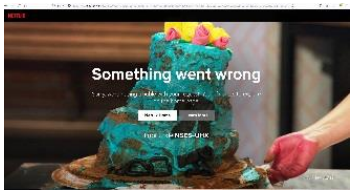
(A Sample Gallery of Spectrum Connection Errors)

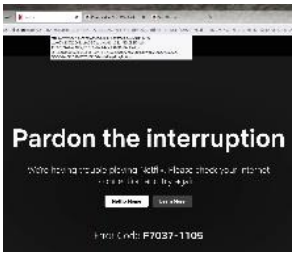
Assorted Insufficient Bandwidth Error Messages (mostly Netflix and Prime Video) as well as the Inadequate Speed Test Results that Follow

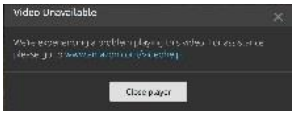



How do I fix page crashes and other page loading errors?
Aw, Snap!
Reload the page
Further troubleshooting
Check your Internet connection







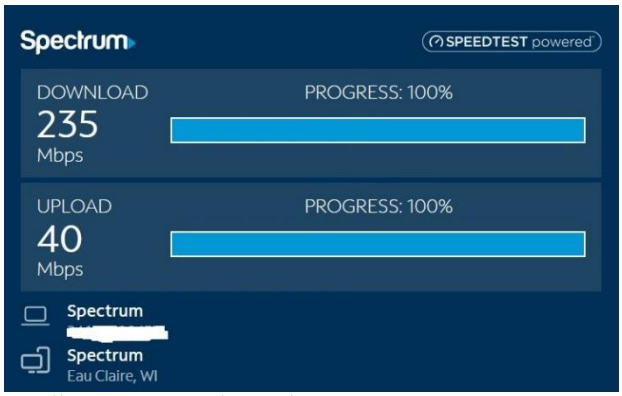


Your device's available Internet bandwidth is too low for uninterrupted streaming, or is experiencing intermittent connectivity. The video might pause while buffering.
Don't show again

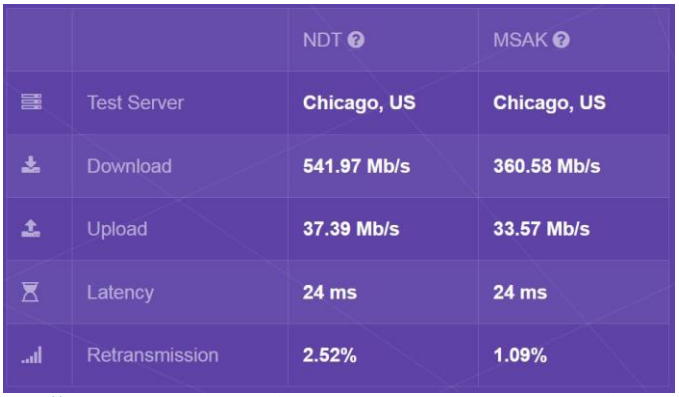
Appendix Two Speed Tests

Speed tests (one through six)

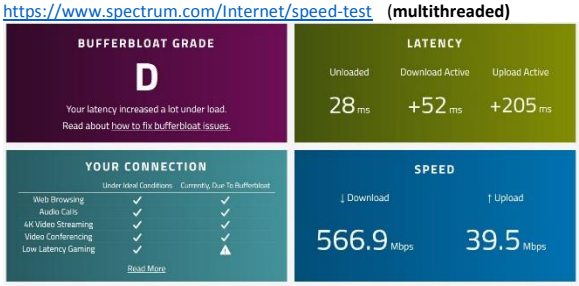
Network: Netgear Nighthawk RAXE500 2.5 Gbps router, 2 - 2.5 Gbps Zyxel switches in series, a 2.5 Gbps Hitron cable modem, 200 ft. Cat 6 Ethernet runs, Cat 7 patch cables



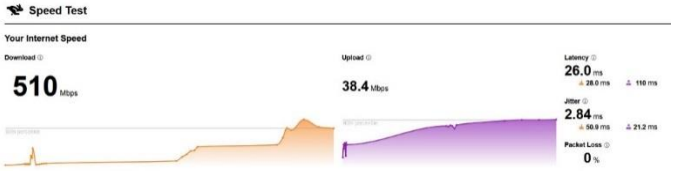
https://www.spectrum.com/Internet/speed-test **(multithreaded)**



https://speed.measurementlab.net **(NDT single threaded, MSAK multithreaded)**



https://www.waveform.com/tools/bufferbloat **(single threaded)**



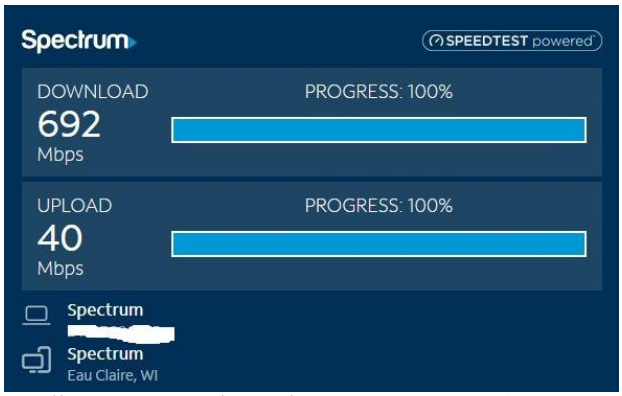
https://speed.cloudflare.com **(single threaded)**

Client: Core i7 desktop Windows 7 Ultimate, 2.5 Gbps network adaptor, Firefox Browser

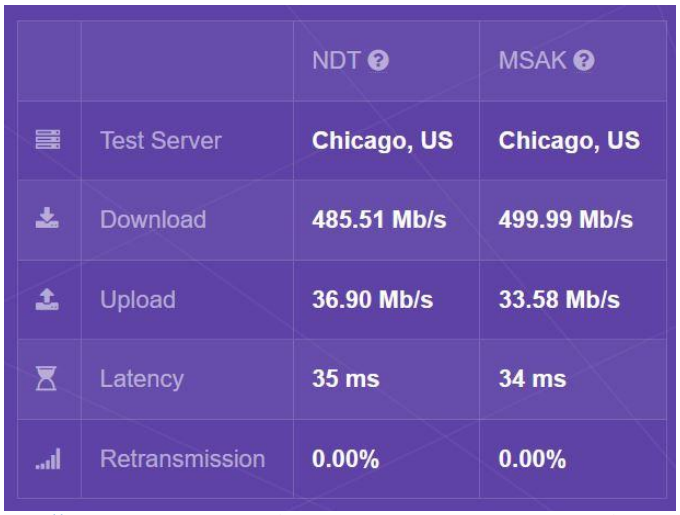
443/38 Mbps Average from a Charter/Spectrum 1000/35 Mbps speed tier, September 30, 2024 (hyperlinks are active)

Note: At no point has a 1000 Mbps speed test been achieved. A majority of speed tests are not linear (single threaded) but multithreaded (which can hide network congestion) and do not test to a relevant IXP, but rather a local ISP node which is not truly indicative of a user experience.

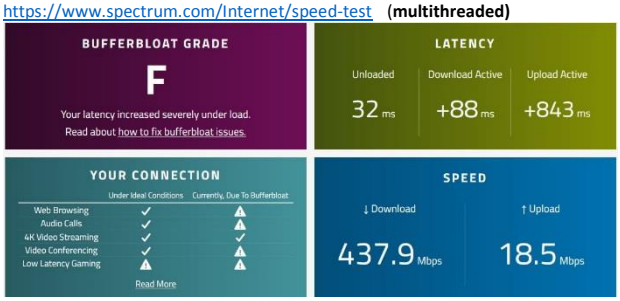
Network: Netgear Nighthawk RAXE500 2.5 Gbps router, 2 - 2.5 Gbps Zyxel switches in series, 2.5 Gbps Hitron cable modem, 200 ft. Cat 6 Ethernet runs, Cat 7 patch cables



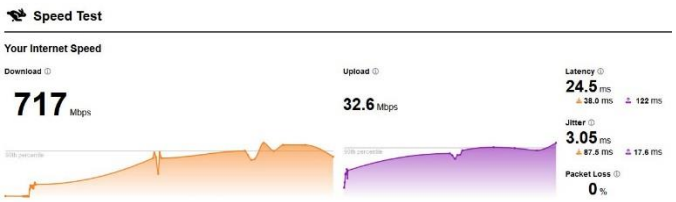
https://www.spectrum.com/Internet/speed-test **(multithreaded)**



https://speed.measurementlab.net **(NDT single threaded, MSAK multithreaded)**



https://www.waveform.com/tools/bufferbloat **(single threaded)**



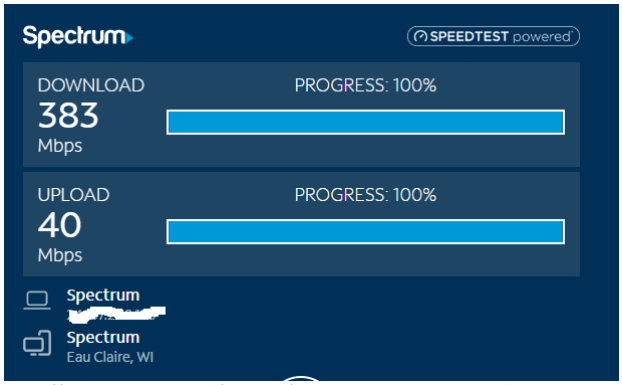
https://speed.cloudflare.com **(single threaded)**

Client: Dell Latitude 3150 laptop Windows 10 22H2, 1 Gbps network adaptor, Firefox Browser

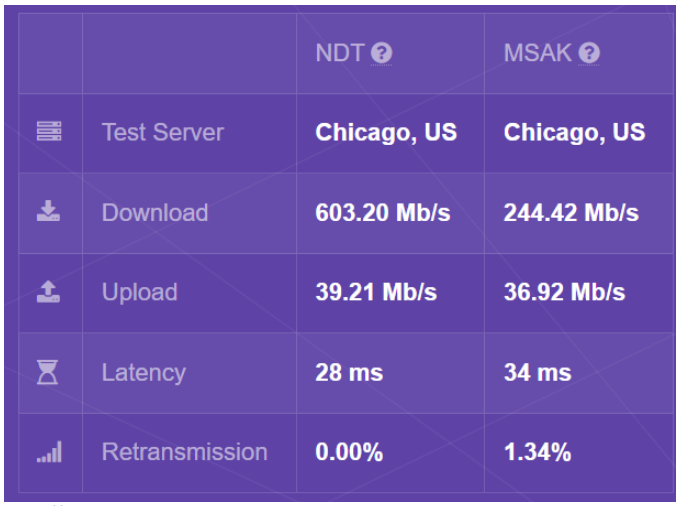
567/32 Mbps Average from a Charter/Spectrum 1000/35 Mbps speed tier, September 29, 2024 (hyperlinks are active)

Note: At no point has a 1000 Mbps speed test been achieved. A majority of speed tests are not linear (single threaded) but multithreaded (which can hide network congestion) and do not test to a relevant IXP, but rather a local ISP node which is not truly indicative of a user experience.

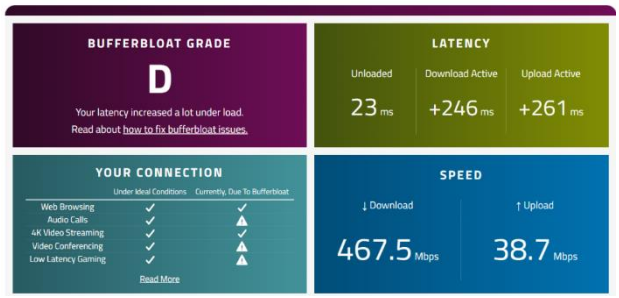
Network: Netgear Nighthawk RAXE500 2.5 Gbps router, 2 - 2.5 Gbps Zyxel switches in series, 2.5 Gbps Hitron cable modem, 200 ft. Cat 6 Ethernet runs, Cat 7 patch cables



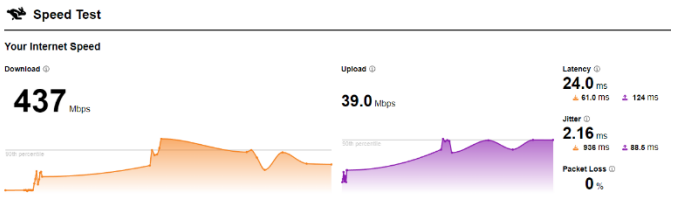
https://www.spectrum.com/Internet/speed-test **(multithreaded)**



https://speed.measurementlab.net **(NDT single threaded, MSAK multithreaded)**



https://www.waveform.com/tools/bufferbloat **(single threaded)**



https://speed.cloudflare.com **(single threaded)**

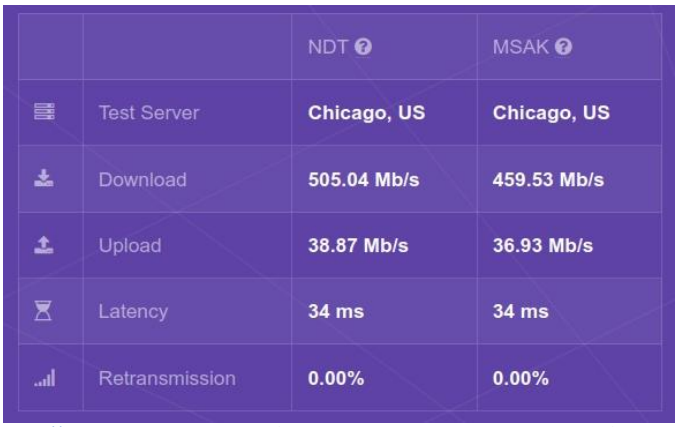
Client: HP ZBook G3 workstation laptop Windows 11 23H2, 2.5 Gbps adaptor, Brave Browser

427/39 Mbps from a Charter/Spectrum 1000/35 Mbps speed tier, September 24, 2024 (hyperlinks are active)

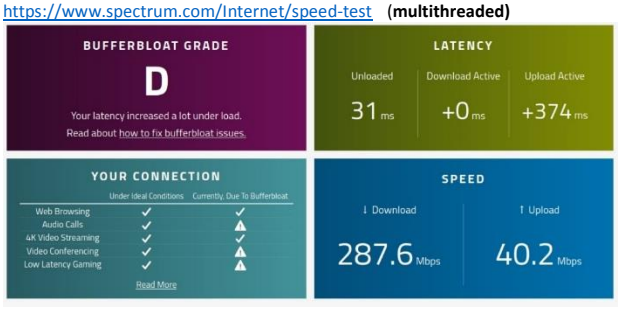
Note: At no point has a 1000 Mbps speed test been achieved. A majority of speed tests are not linear (single threaded) but multithreaded (which can hide network congestion) and do not test to a relevant IXP, but rather a local ISP node which is not truly indicative of a user experience.

Network: Netgear Nighthawk RAXE500 2.5 Gbps router, 2 - 2.5 Gbps Zyxel switches, 2.5 Gbps, a Hitron cable modem, 200 ft. Cat 6 Ethernet runs, Cat 7 patch cables

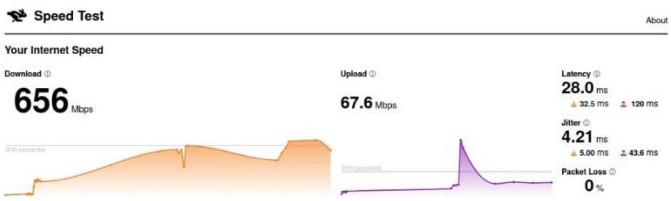
https://www.spectrum.com/Internet/speed-test **(multithreaded)**



https://speed.measurementlab.net **(NDT single threaded, MSAK multithreaded)**



https://www.waveform.com/tools/bufferbloat **(single threaded)**



https://speed.cloudflare.com **(single threaded)**

Client: Core i7 desktop Linux Mint 21.2 Victoria, 1 Gbps network adaptor, Firefox Browser

568/44 Mbps Average from a Charter/Spectrum 1000/35 Mbps speed tier, September 30, 2024 (hyperlinks are active)

Note: At no point has a 1000 Mbps speed test been achieved. A majority of speed tests are not linear (single threaded) but multithreaded (which can hide network congestion) and do not test to a relevant IXP, but rather a local ISP node which is not truly indicative of a user experience.

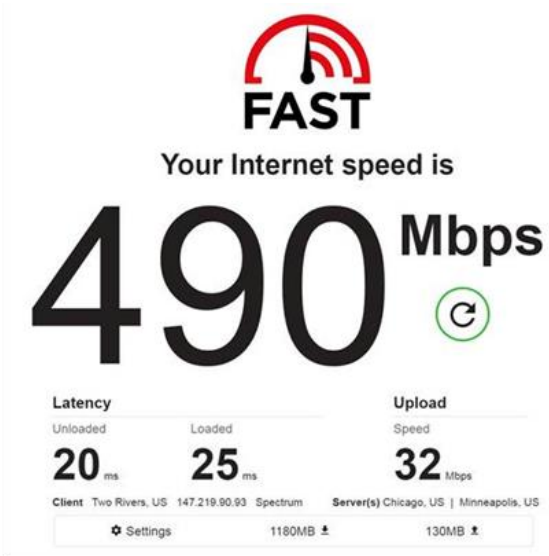
Appendix Three VPN's

VIRTUAL PRIVATE NETWORK (VPN) PERFORMANCE - 1

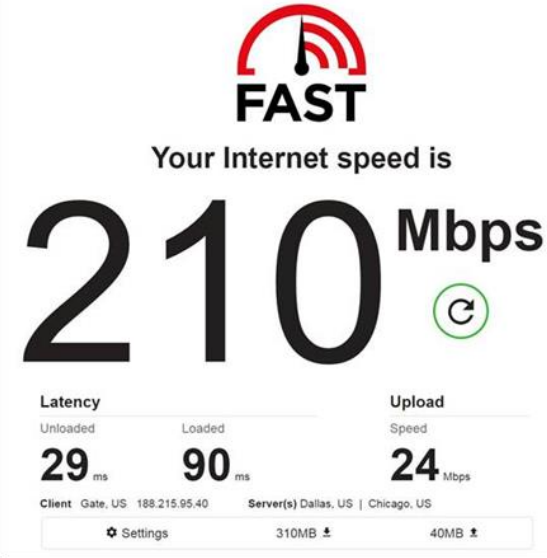
Charter/Spectrum 1000 Mbps speed tier, October 17, 2024

Network: Netgear Nighthawk RAXE500 2.5 Gbps router, 2 - 2.5 Gbps Zyxel switches, 2.5 Gbps Hitron cable modem (200 ft. Cat 6 Ethernet run, Cat 7 patch cables)

Two Rivers to Chicago normal connection



VPN from Dallas to the same site in Chicago



Client: Core i7 desktop Windows 7 Ultimate, 2.5 Gbps network adaptor, Firefox Browser, ExpressVPN

Note: ExpressVPN uses several protocols to ensure secure, fast, and reliable connections. These are the main protocols used by ExpressVPN:

Lightway: This is ExpressVPN's proprietary protocol, designed for speed and security. It is lightweight, fast, and optimized for mobile devices, with low battery consumption. It is a modern, open-source protocol built to improve upon older VPN protocols.

OpenVPN: A widely used, open-source protocol that is known for its strong security. It supports both UDP (User Datagram Protocol) and TCP (Transmission Control Protocol) for data transmission. OpenVPN is considered very secure but may be slower than Lightway in some cases.

WireGuard: A newer, high-performance VPN protocol that has gained popularity for its speed and simplicity. ExpressVPN supports WireGuard-based protocols (like IKEv2/IPSec) to ensure efficient encryption with minimal latency.

IKEv2/IPSec: Known for its speed and stability, this protocol is often used for mobile devices because of its ability to quickly reconnect after a connection drop (e.g., switching between Wi-Fi and mobile networks).

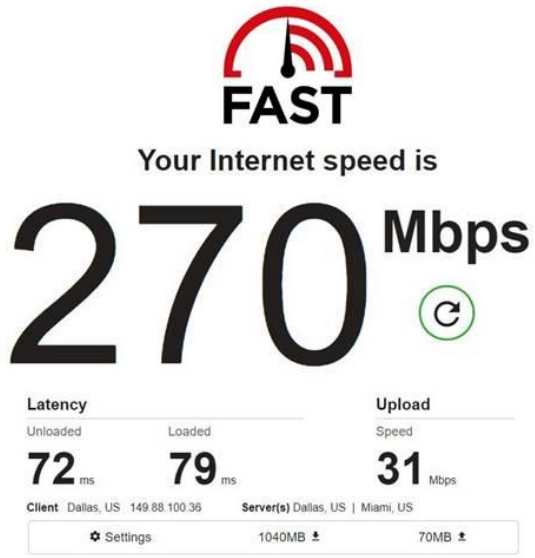
L2TP/IPSec: While not as secure or fast as OpenVPN or WireGuard, this protocol is still commonly used for compatibility with various devices. It offers a balance of security and speed but is considered less secure than newer protocols.

ExpressVPN automatically selects the best protocol based on the network conditions and device you're using, though you can manually choose one of these protocols in the app settings.

VIRTUAL PRIVATE NETWORK (VPN) PERFORMANCE - 2
Charter/Spectrum 1000 Mbps speed tier, October 17, 2024
Network: Netgear Nighthawk RAXE500 2.5 Gbps router, 2 - 2.5 Gbps Zyxel switches, 2.5 Gbps Hitron cable modem (200 ft. Cat 6 Ethernet run, Cat 7 patch cables)

Two Rivers to Chicago normal connection

VPN from USA Central to the same site in Chicago



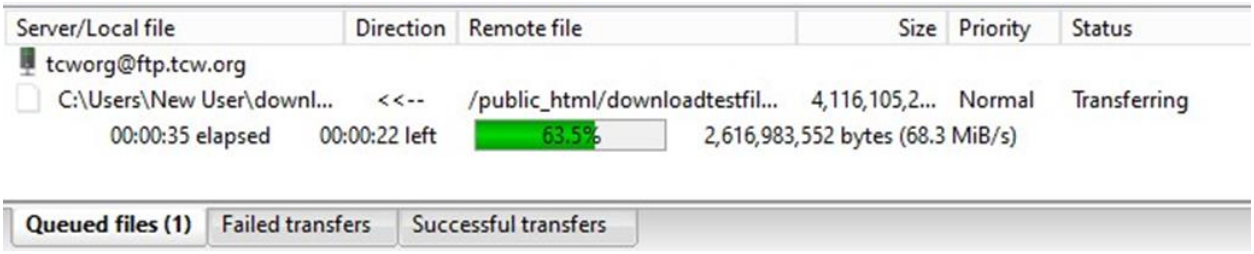
Client: HP ZBook G3 workstation laptop Windows 11 23H2, 2.5 Gbps adaptor, Brave Browser VPN

Note: Brave VPN, which is integrated into the Brave browser, primarily uses the WireGuard protocol. WireGuard is known for its speed, simplicity, and strong security. It is a modern VPN protocol that provides efficient encryption with minimal latency and is widely regarded as one of the most secure and fast VPN protocols available.
Brave VPN, leveraging WireGuard, ensures a good balance between performance and privacy, offering users a fast and secure browsing experience while protecting their data.

See Appendix for more information on VPN's

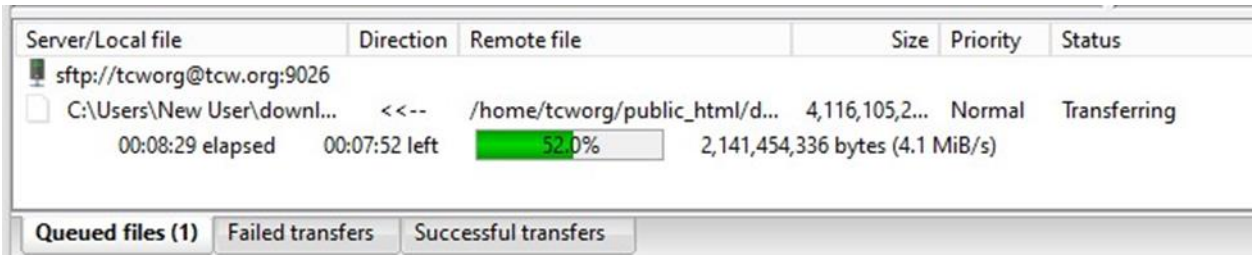
Appendix Four Beyond Speed Test Sites (FTP)

Internet speed tests are in reality, a multi-second test at a specific point in time. Speed tests, some to an IXP backbone Internet connection or CDN, and some just to a local **Intranet** node. Some are longer or shorter, some single threaded or linear, and some multi-threaded making relevance questionable and relegating them to beauty contests for ISP marketing and useful to consumers only for comparison purposes. I set out to find out my actual Quality of Internet Experience, or QoE, is.



572Mbps FileZilla FTP download from my website hosting server in Milwaukee

Just as is the case with severely reduced bandwidth with a VPN encryption connection, if I use Secure FTP, or SFTP, the results are much worse. Now, any secure connection is going to add overhead as each packet needs to be decrypted on the server, however a VPN encrypt/decrypt overhead is typically 10-20%.



34 Mbps FileZilla SFTP download from my website hosting server in Milwaukee

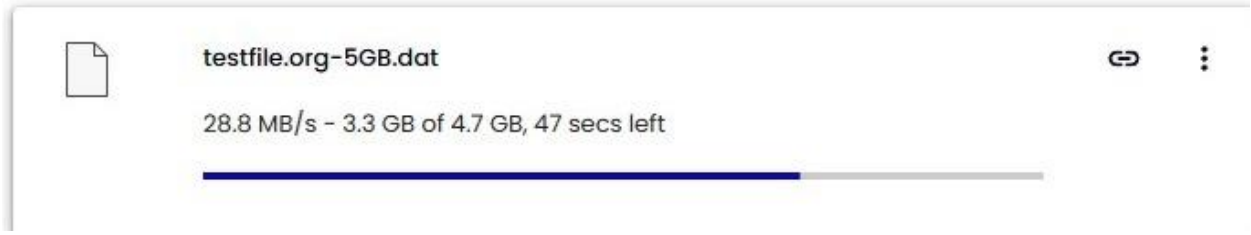
Not accounting for time of day network activity, 3am on a Sunday versus 9am on a Monday, I got the above results: 572 Mbps FTP versus 34 Mbps SFTP. 34 is a 94% decrease of 572, which is a significant difference.

It is nearly impossible to determine if these results are due to congestion on the hosting server network or ISP network that account for this performance delta. If past tests are precedent, it is congestion of the ISP network that is the cause of my poor VPN results, and so likely with SFTP as well.

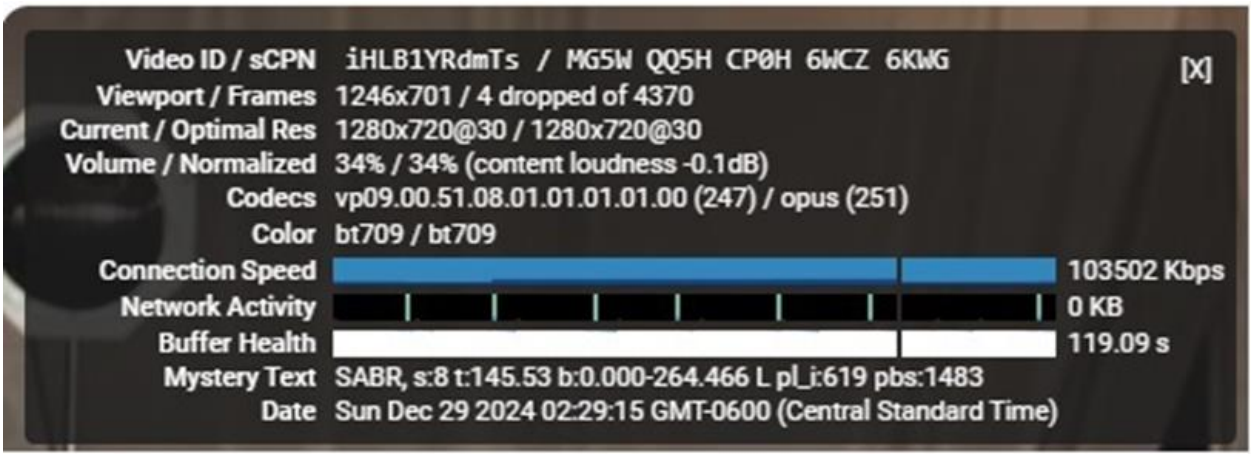
This is supported by the fact that SFTP is basically file transfer over Secure Shell Protocol or SSH, and my speed tests to the secure hosting network, https://www.hostingsupport.io, are within the range of my other speed tests on the Charter/Spectrum Intranet (SpectrumNet). This logically and based on factual evidence, leaves the ISP network Charter/Spectrum, as the most likely culprit.

See Appendix for more information on FTP/SFTP

QoE testing continued…



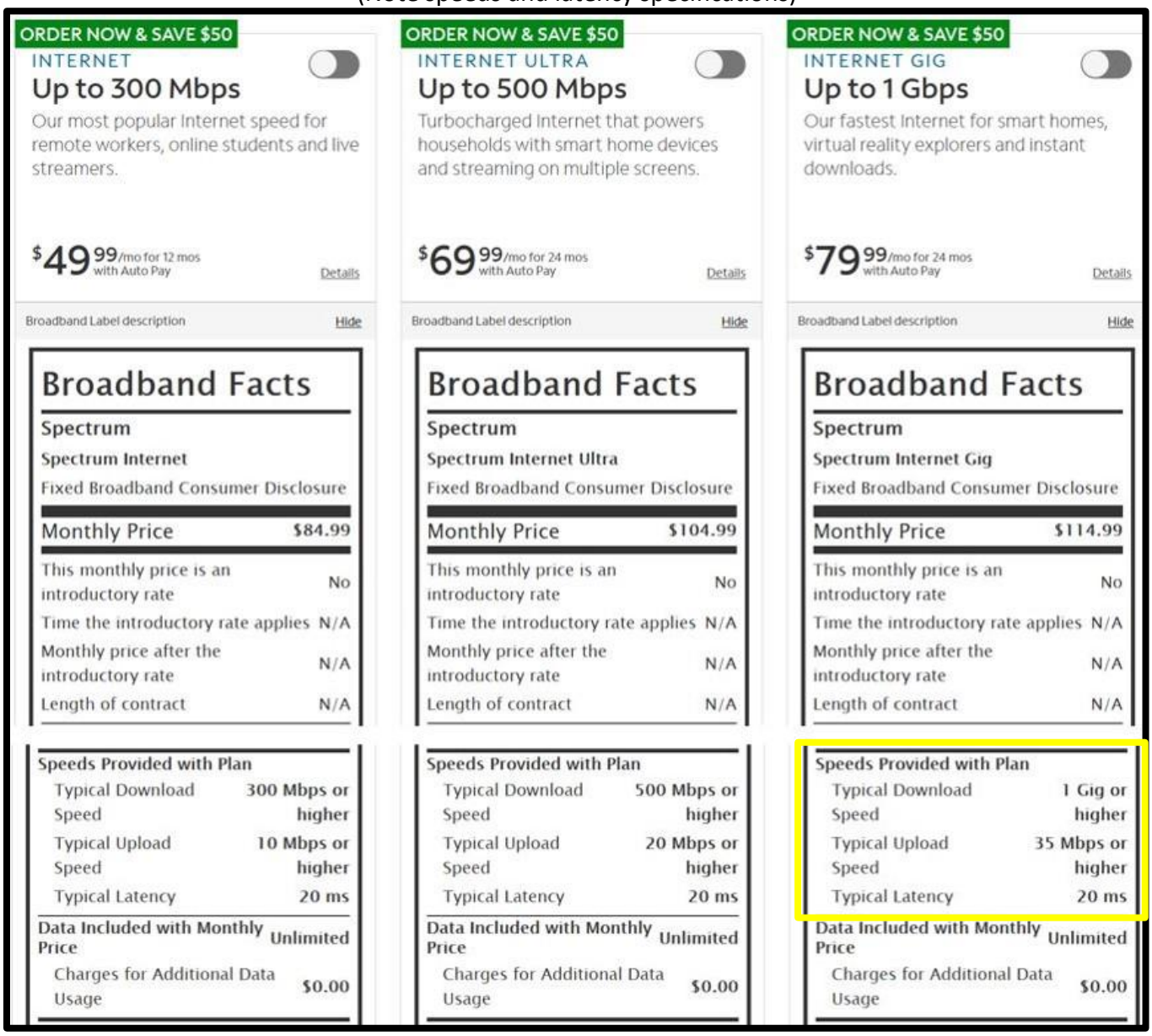
230 Mbps test file download from testfile.org via Minneapolis MICE to CloudFlare in San Francisco


Video ID / sCPN iHLB1YRdmTs / MG5W QQ5H CP0H 6WCZ 6KWG
[X]
Viewport / Frames 1246x701 / 4 dropped of 4370
Current / Optimal Res 1280x720@30 / 1280x720@30
Volume / Normalized 34% / 34% (content loudness -0.1dB)
Codecs vp09.00.51.08.01.01.01.01.00 (247) / opus (251)
Color bt709 / bt709
Connection Speed 103502 Kbps
Network Activity 0 KB
Buffer Health 119.09 s
Mystery Text SABR, s:8 t:145.53 b:0.000-264.466 L pl_i:619 pbs:1483
Date Sun Dec 29 2024 02:29:15 GMT-0600 (Central Standard Time)

103.502 Mbps YouTube streaming download speed via Chicago, to (DCH) Data Center/Web Hosting/Transit Google in Atlanta

Testing details:
Network: Netgear Nighthawk RAXE500 2.5 Gbps router, Qty. 2 - 2.5 Gbps Zyxel switches in series, a 2.5 Gbps Hitron cable modem (200 ft. Cat 6 Ethernet runs, Cat 7 patch cables)
Client: HP ZBook G3 workstation laptop Windows 11 23H2, using factory 1 Gbps network adaptor, Brave Browser
Charter/Spectrum HFC 1000/35 Mbps speed tier, December 29, 2024 3AM

Appendix Five Bandwidth Labels
FCC Required Advertising That Conflicts With Reality
(Note speeds and latency specifications)



ORDER NOW & SAVE $50

INTERNET
Up to 300 Mbps
Our most popular Internet speed for remote workers, online students and live streamers.
$49.99/mo for 12 mos with Auto Pay
Details

Broadband Label description Hide

Broadband Facts

Spectrum
Spectrum Internet
Fixed Broadband Consumer Disclosure

Monthly Price	$84.99
This monthly price is an introductory rate	No
Time the introductory rate applies	N/A
Monthly price after the introductory rate	N/A
Length of contract	N/A

Speeds Provided with Plan	
Typical Download Speed	300 Mbps or higher
Typical Upload Speed	10 Mbps or higher
Typical Latency	20 ms
Data Included with Monthly Price	Unlimited
Charges for Additional Data Usage	$0.00

ORDER NOW & SAVE $50

INTERNET ULTRA
Up to 500 Mbps
Turbocharged Internet that powers households with smart home devices and streaming on multiple screens.
$69.99/mo for 24 mos with Auto Pay
Details

Broadband Label description Hide

Broadband Facts

Spectrum
Spectrum Internet Ultra
Fixed Broadband Consumer Disclosure

Monthly Price	$104.99
This monthly price is an introductory rate	No
Time the introductory rate applies	N/A
Monthly price after the introductory rate	N/A
Length of contract	N/A

Speeds Provided with Plan	
Typical Download Speed	500 Mbps or higher
Typical Upload Speed	20 Mbps or higher
Typical Latency	20 ms
Data Included with Monthly Price	Unlimited
Charges for Additional Data Usage	$0.00

ORDER NOW & SAVE $50

INTERNET GIG
Up to 1 Gbps
Our fastest Internet for smart homes, virtual reality explorers and instant downloads.
$79.99/mo for 24 mos with Auto Pay
Details

Broadband Label description Hide

Broadband Facts

Spectrum
Spectrum Internet Gig
Fixed Broadband Consumer Disclosure

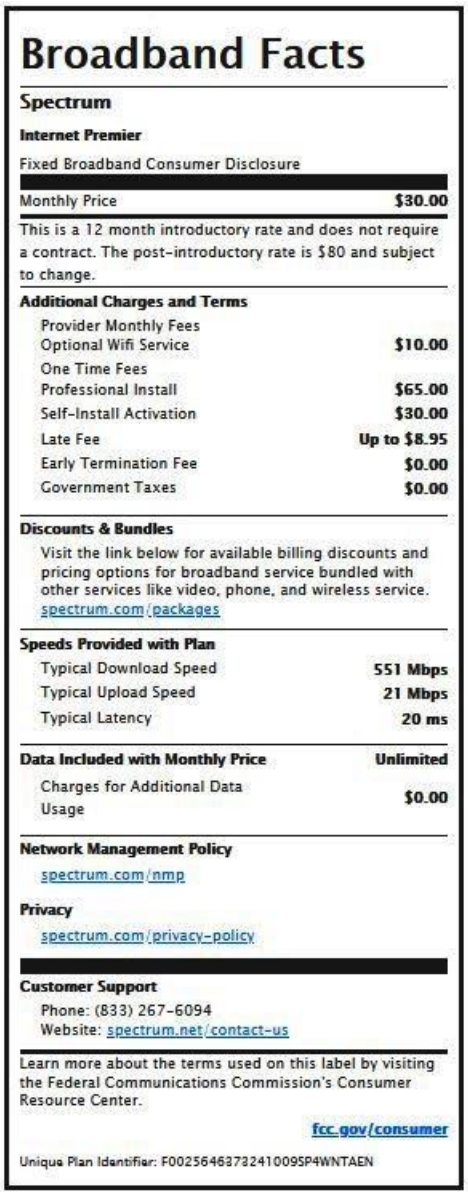
Monthly Price	$114.99
This monthly price is an introductory rate	No
Time the introductory rate applies	N/A
Monthly price after the introductory rate	N/A
Length of contract	N/A

Speeds Provided with Plan	
Typical Download Speed	1 Gig or higher
Typical Upload Speed	35 Mbps or higher
Typical Latency	20 ms
Data Included with Monthly Price	Unlimited
Charges for Additional Data Usage	$0.00

Note: My broadband label says 1 Gbps or higher download, 35 Mbps or higher upload and 20 ms typical latency. My averaged results across four machines, four OS's, and two browsers on a full 2.5 Gbps network is 501 Mbps download, 38 upload, and an average latency of 30 ms (although 60 ms RTT pings from trace routes are not uncommon)
So what good are these labels really?

My Former Address That Now Has Fiber (as you can see below)

Spectrum



Broadband Facts

Spectrum

Internet Premier

Fixed Broadband Consumer Disclosure

Monthly Price	$30.00

This is a 12 month introductory rate and does not require a contract. The post-introductory rate is $80 and subject to change.

Additional Charges and Terms

Provider Monthly Fees	
Optional Wifi Service	$10.00
One Time Fees	
Professional Install	$65.00
Self-Install Activation	$30.00
Late Fee	Up to $8.95
Early Termination Fee	$0.00
Government Taxes	$0.00

Discounts & Bundles

Visit the link below for available billing discounts and pricing options for broadband service bundled with other services like video, phone, and wireless service.
spectrum.com/packages

Speeds Provided with Plan

Typical Download Speed	551 Mbps
Typical Upload Speed	21 Mbps
Typical Latency	20 ms

Data Included with Monthly Price	**Unlimited**
Charges for Additional Data Usage	$0.00

Network Management Policy

spectrum.com/nmp

Privacy

spectrum.com/privacy-policy

Customer Support

Phone: (833) 267-6094
Website: spectrum.net/contact-us

Learn more about the terms used on this label by visiting the Federal Communications Commission's Consumer Resource Center.

fcc.gov/consumer

Unique Plan Identifier: F00256463732410095P4WNTAEN

Broadband Facts

Spectrum

Internet Gig

Fixed Broadband Consumer Disclosure

Monthly Price	$50.00

This is a 12 month introductory rate. The post-introductory rate is $100 and subject to change. Modem and Advanced Wifi service included.

Additional Charges and Terms

Provider Monthly Fees	
Optional Wifi Service	$0.00
One Time Fees	
Professional Install	$65.00
Self-Install Activation	$30.00
Late Fee	Up to $8.95
Early Termination Fee	$0.00
Government Taxes	$0.00

Discounts & Bundles

Visit the link below for available billing discounts and pricing options for broadband service bundled with other services like video, phone, and wireless service.
spectrum.com/packages

Speeds Provided with Plan

Typical Download Speed	1064 Mbps
Typical Upload Speed	1025 Mbps
Typical Latency	20 ms

Data Included with Monthly Price	**Unlimited**
Charges for Additional Data Usage	$0.00

Network Management Policy

spectrum.com/nmp

Privacy

spectrum.com/privacy-policy

Customer Support

Phone: (833) 267-6094
Website: spectrum.net/contact-us

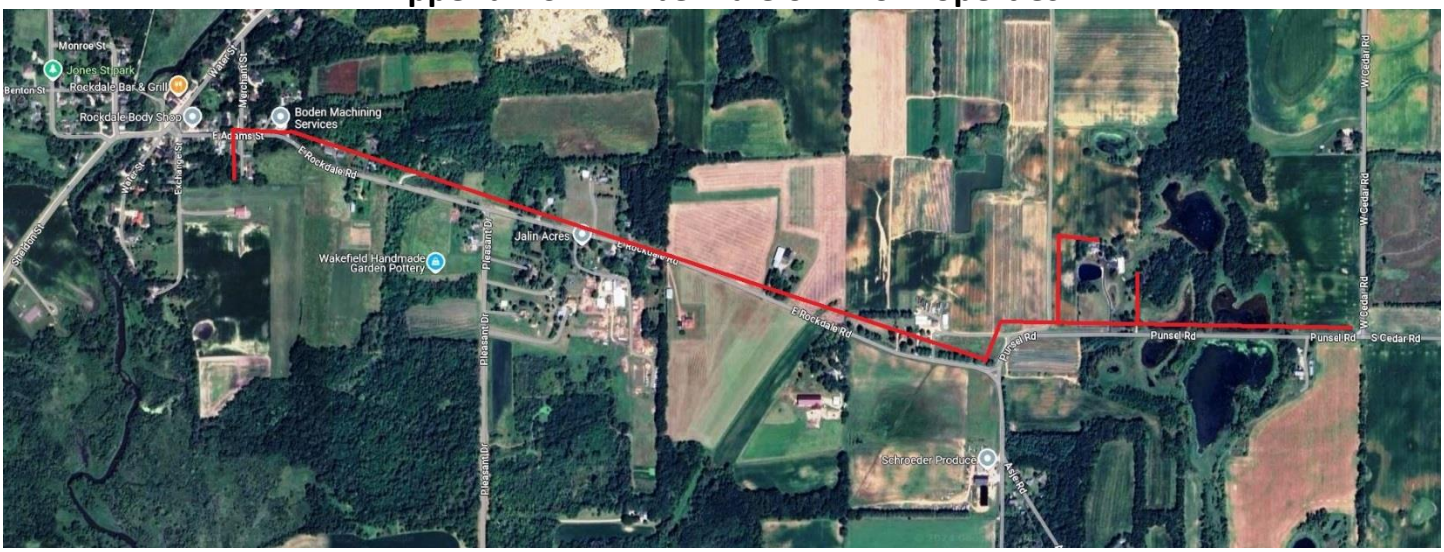
Learn more about the terms used on this label by visiting the Federal Communications Commission's Consumer Resource Center.

fcc.gov/consumer

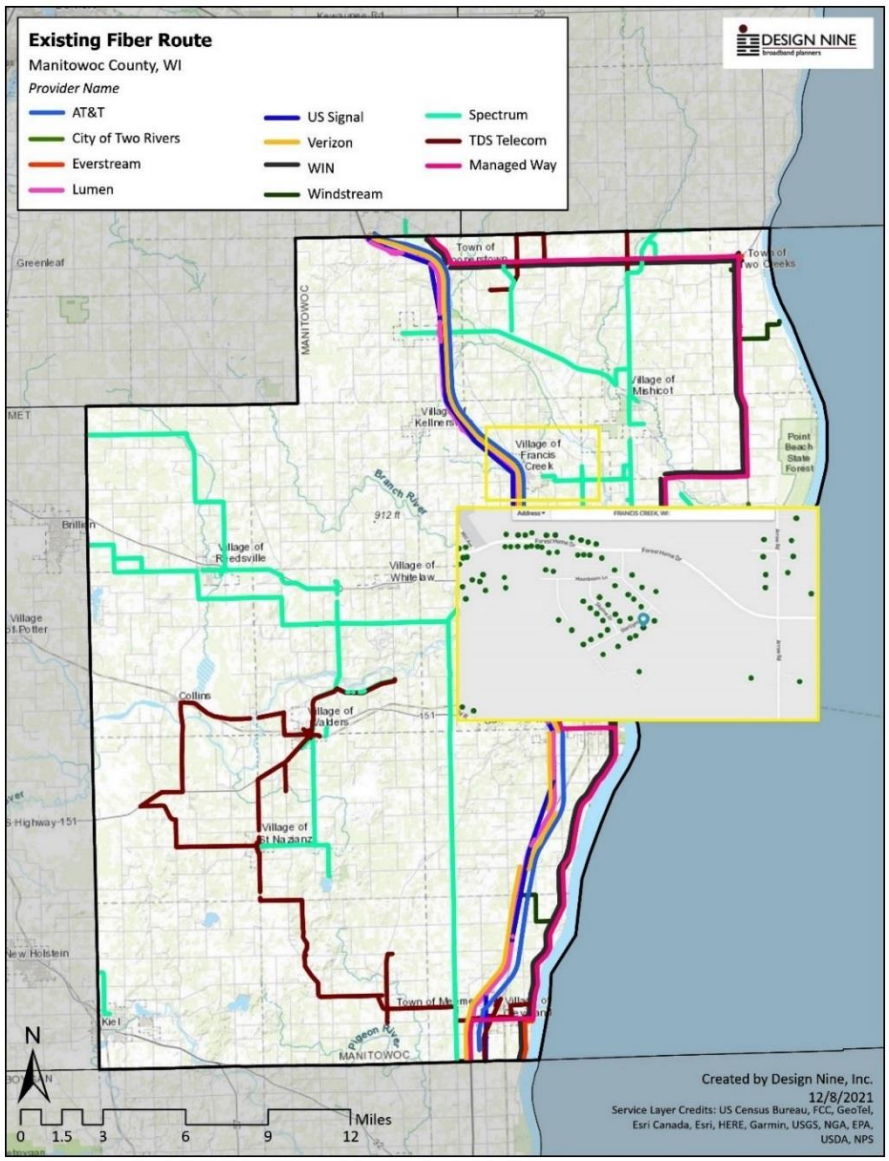
Unique Plan Identifier: F00256463732410095G4WNTSEN

Notice how they unnecessarily throttle the upload speed on the Premier connection. Perhaps a ploy to get the social media people to upgrade. Also note the high latency which is unheard of for fiber. It ordinarily should be less than 5 ms.

Appendix Six A Fiber Tale of Two Properties



If Charter/Spectrum can lay fiber optic cable in the rural country here. 1054/1025 Mbps $50/12 mo. then $100/mo.



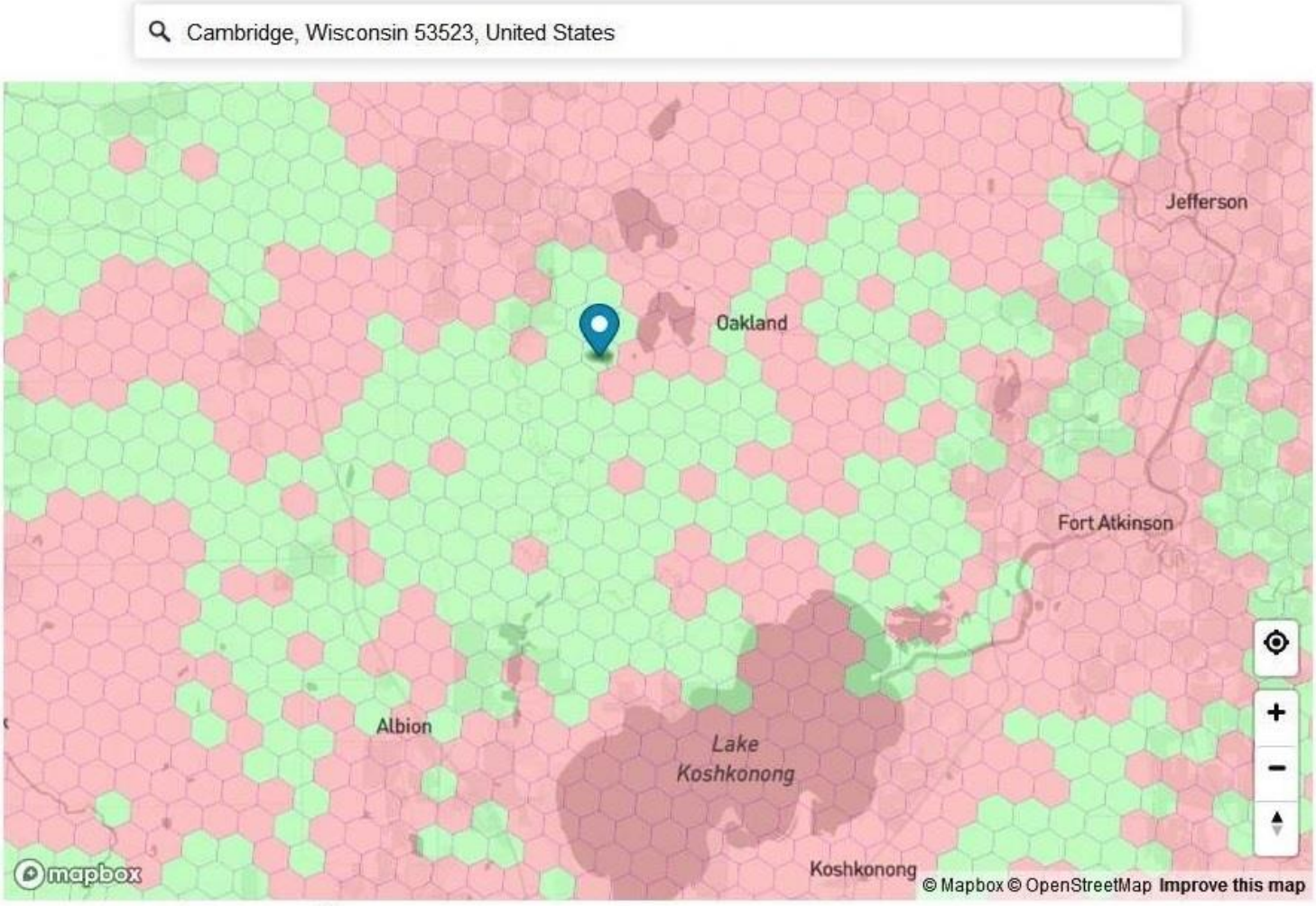
Why can’t OR won’t they lay fiber to a subdivision here?

A Fiber Tale of Two Properties (cont)

And then there is the seemingly random nature of the fiber deployments.

Spectrum Fiber Availability Map

Green hexagons show where Spectrum services at least one address with fiber internet.



Data Sourcing

Availability data for Spectrum comes from the FCC's Broadband Data Collection program.

Charter/Spectrum will likely never lay fiber optic cable in my subdivision because they are already getting $108 mo. from me for 1000/35 Mbps HFC, which in reality is more like 500/30 Mbps, and they can't justify spending many thousands of dollars to lay fiber to be able to get $100/mo. from me.

They have already captured me in their monopoly web (trough) of despair.

- Monopolization leads to stagnation, which is why we are 25 years down the road without fiber everywhere.
- Competition leads to innovation, and better offerings to customers. See Project Utopia in Utah. Differentiation could be offerings of not just lame phone and TV add-ons but home mesh networks, Ethernet cable installations, flexible service and pricing plans, improved support etc.
- The fiber running down the county road past my subdivision should be owned by the county and leased to at least several Internet providers.

Appendix Six VPN's (continued)

Some Details of Encryption Overhead in a VPN Connection

A VPN encrypts the entire network traffic between your device and the VPN server. This can include all applications (web browsing, file transfers, email, etc.) running over the VPN connection. VPNs use protocols like OpenVPN, IPsec, WireGuard, etc., and the encryption typically uses AES or similar algorithms which create the bandwidth and latency overheads of maintaining the VPN tunnel and handling all switched packets.

VPN protocols may also employ compression. Compression can reduce the effective bandwidth usage, but the overhead of encrypting the entire traffic stream may actually make VPNs consume more bandwidth.

Overhead

- The encryption overhead in VPNs is because it encrypts and decrypts all network traffic.
- VPN encryption happens at the network layer, affecting the entire data flow, so the overhead depends on the VPN protocol and the amount of data being transmitted across the VPN.

Performance

- VPNs can introduce noticeable latency and reduced throughput, especially with high traffic or using less efficient encryption protocols.
- VPNs may also be affected by network factors such as ***packet loss, routing, and congestion***, which can further increase overhead.
- VPNs, depending on the protocol and encryption level, can have a 20% to 40% or more overhead on bandwidth. The reason for this higher overhead is that VPNs encrypt all network traffic, including headers, and manage the tunneling of all data packets.
- For a 100 Mbps connection and you use a VPN with a 30% overhead, the effective bandwidth available for actual data transmission might drop to 70 Mbps due to the encryption overhead.
- For a 1000 Mbps connection, a VPN might use between 600 Mbps and 800 Mbps for total traffic, depending on the encryption strength and the VPN protocol.

Some Details Regarding VPN Congestion

VPNs operate by creating a secure tunnel for all network traffic, including web browsing, email, file transfers, and any other applications. The impact of network congestion on a VPN is complex because it affects all traffic passing through the VPN tunnel.

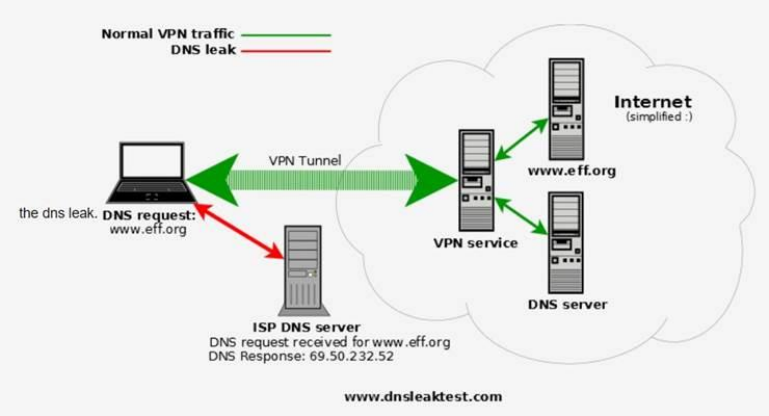
Response to Congestion

- Latency and Speed: Network congestion will increase latency and decrease throughput for all traffic passing through the VPN. This includes not only file transfers but also all other applications and services that use the VPN. Since the VPN encrypts and encapsulates all packets, congestion can cause overall network slowdown, as the entire VPN tunnel becomes a bottleneck.
- TCP and UDP Behavior: If the VPN is using TCP (e.g., OpenVPN), it inherits TCP's congestion control mechanisms. For UDP-based VPNs (e.g., WireGuard), congestion may still result in packet loss, but there are no retransmissions like with TCP. UDP VPNs may experience more packet loss and higher delays when the network is congested.

- Tunnel Overhead: VPNs introduce additional overhead for encapsulating and encrypting traffic. During congestion, this added overhead could exacerbate the reduction in throughput because the network needs to handle both the original data and the encapsulation overhead.
- Increased Latency for All Traffic: VPN congestion impacts all data in the VPN tunnel, including web browsing, video streaming, VoIP calls, and file transfers will all experience slowdowns and latency increases.

Congestion Effects on VPN Protocol: Some VPN protocols are more robust than others under congestion. For example, WireGuard tends to perform better under network stress due to its lightweight and efficient design, while OpenVPN (especially with TCP) may struggle more under heavy congestion.

Note: Ran some tests on https://routersecurity.org and https://dnsleaktest.com and discovered that the Brave browser VPN appears to leak.



Ran this same test on ExpressVPN and no leakage.

Appendix Eight - FTP/SFTP - File Transfers

Secure FTP (SFTP:\\domainname.domaintype)

SFTP (Secure File Transfer Protocol)

SFTP operates over **SSH** (Secure Shell), and its primary purpose is to securely transfer files. It is a file-specific protocol, and its performance is affected by network congestion, but in a more localized and specific way compared to VPNs.

- **Response to Congestion**:
  - **Latency and Speed**: When the network is congested, **SFTP** may experience **increased latency** and **slower transfer speeds**. Since SFTP handles file transfers, it is sensitive to delays in the network, which can affect the overall speed of the file transfer. The speed typically decreases linearly with congestion, and files will take longer to transfer due to lower throughput.
  - **TCP Congestion Control**: SFTP uses TCP as its transport protocol, meaning it relies on **TCP's congestion control mechanisms** (e.g., slow start, congestion window adjustments). This allows SFTP to **throttle** its transmission rate during congestion and avoid overwhelming the network further, but it also means SFTP transfers may slow down or stall temporarily if congestion is severe.
  - **Retransmissions**: Network congestion can lead to **packet loss**, and when this happens, TCP will **retransmit lost packets**. This retransmission process further slows down file transfer speeds, especially for large files.
  - **Impact on Other Traffic**: SFTP only affects the **file transfer traffic**. If there is congestion, other network applications or services (like web browsing or VoIP) may still operate normally unless the congestion is so severe that it impacts overall available bandwidth.

Summary for SFTP:

- **Impact**: Increased congestion leads to slower file transfer speeds and potentially longer wait times for completion.
- **Recovery**: SFTP relies on TCP's congestion control to adapt, but can be slower to recover from congestion compared to more dynamic protocols.
- **Localized Impact: Only affects file transfers, not the whole network.**
- **Encryption Mechanism: SFTP is based on SSH (Secure Shell) and encrypts file data during transfer. It ensures data confidentiality and integrity but only for the files being transferred. The encryption typically uses algorithms like AES (Advanced Encryption Standard) or similar.**

- **Overhead**:
  - The encryption overhead in SFTP comes from the encryption and decryption processes applied to the individual file transfers.
  - The more files transferred, the more CPU and bandwidth are consumed for encryption and decryption.

    - Since SFTP encrypts data at the application layer (on a per-file basis), the overhead is relatively lower than that of a full network layer encryption like VPN.
- **Performance**:
    - SFTP can suffer from latency due to the handshakes involved in establishing the secure connection and the need to encrypt the entire file stream.
    - It might experience some performance degradation depending on the file size and network conditions, but the overhead is mostly contained to the file transfer sessions.

General Bandwidth Overhead Estimates

- **SFTP**:
    - The overhead of SFTP encryption is typically between **5% to 20%** of the total bandwidth, depending on the encryption algorithm used (e.g., AES-128 vs AES-256) and the size of the files. The larger the file being transferred, the lower the relative overhead, because the fixed cost of encryption is amortized over more data.
    - For example, if you are transferring a 100 MB file with 10% encryption overhead, the actual bandwidth used might be **110 MB**.

Estimates for Bandwidth Usage (in Mbps)

- **SFTP**:
    - If you're using **SFTP** over a 100 Mbps link, and assuming the encryption overhead is about **10%**, you might see around **90 to 95 Mbps** being available for actual file transfers (after encryption).

SFTP Bandwidth Usage Estimate (1000 Mbps Connection)

- **SFTP Overhead**: As mentioned earlier, SFTP encryption overhead is generally in the range of **5% to 20%**.
    - **Low Estimate (5% Overhead)**: If the overhead is on the lower end (5%), then:
        - Usable bandwidth for file transfers = **1000 Mbps - 5% of 1000 Mbps = 1000 Mbps - 50 Mbps = 950 Mbps**.
    - **High Estimate (20% Overhead)**: If the overhead is on the higher end (20%), then:
        - Usable bandwidth for file transfers = **1000 Mbps - 20% of 1000 Mbps = 1000 Mbps - 200 Mbps = 800 Mbps**.

Appendix Nine - Wisconsin Statute Annotated § 66.0422

Wisconsin state laws allow municipalities to own and operate broadband networks, but such networks can only be paid for by subscribers of the service, not the general population. Municipalities are required to conduct feasibility studies and hold public hearings prior to offering service, allowing telecom incumbents ample opportunity to stall broadband projects. Public entities must include phantom costs in their rates and are not able to charge rates that are lower than what incumbents charge for the same service. The state laws also prohibit municipalities from subsidizing telecom services**.(See bolded provisions below)**

66.0422 Video service, telecommunications, and broadband facilities.
(1) In this section:
(b) "Local government" means a city, village, or town.
(c) "Telecommunications service" has the meaning given in s. 196.01 (9m).
(d) "Video service" has the meaning given in s. 66.0420 (2) (y).
(2) Except as provided in subs. (3), (3d), (3m), and (3n), no local government may enact an ordinance or adopt a resolution authorizing the local government to construct, own, or operate any facility for providing video service, telecommunications service, or broadband service, directly or indirectly, to the public, unless all of the following are satisfied:
(a) The local government holds a public hearing on the proposed ordinance or resolution.
(b) Notice of the public hearing is given by publication of a class 3 notice under ch. 985 in the area affected by the proposed ordinance or resolution.
(c) No less than 30 days before the public hearing, the local government prepares and makes available for public inspection a report estimating the total costs of, and revenues derived from, constructing, owning, or operating the facility and including a cost-benefit analysis of the facility for a period of at least 3 years. The costs that are subject to this paragraph include personnel costs and costs of acquiring, installing, maintaining, repairing, or operating any plant or equipment, and include an appropriate allocated portion of costs of personnel, plant, or equipment that are used to provide jointly both telecommunications services and other services.
(3) Subsection (2) does not apply to a local government if all of the following conditions apply:
(a) On November 1, 2003, the public service commission has determined that the local government is an alternative telecommunications utility under s. 196.203.
(b) A majority of the governing board of the local government votes to submit the question of supporting the operation of the facility for providing video service, telecommunications service, or Internet access service, directly or indirectly to the public, by the local government to the electors in an advisory referendum and a majority of the voters in the local government voting at the advisory referendum vote to support operation of such a facility by the local government.
(3d) Subsection (2) does not apply to a facility for providing broadband service to an area within the boundaries of a local government if any of the following are satisfied:
(a) The local government asks, in writing, each person that provides broadband service within the boundaries of the local government whether the person currently provides broadband service to the area or intends to provide broadband service within 9 months to the area and within 60 days after receiving the written request no person responds in writing to the local government that the person

currently provides broadband service to the area or intends to provide broadband service to the area within 9 months.
(b) The local government determines that a person who responded to a written request under par. (a) that the person currently provides broadband service to the area did not actually provide broadband service to the area and no other person makes the response to the local government described in par. (a).(c) The local government determines that a person who responded to a written request under par. (a) that the person intended to provide broadband service to the area within 9 months did not actually provide broadband service to the area within 9 months and no other person makes the response to the local government described in par. (a).
(3m) Subsection (2) does not apply to a facility for providing broadband service if all of the following apply:
(a) The municipality offers use of the facility on a nondiscriminatory basis to persons who provide broadband service to end users of the service.
(b) The municipality itself does not use the facility to provide broadband service to end users.
(c) The municipality determines that, at the time that the municipality authorizes the construction, ownership, or operation of the facility, whichever occurs first, the facility *does not* compete with more than one provider of broadband service.
(3n) Subsection (2) does not apply to a local government that, on March 1, 2004, was providing video service to the public.
(4) Notwithstanding sub. (2), a local government may enact an ordinance or adopt a resolution authorizing the local government to prepare a report specified in sub. (2) (c).
(5) If a local government enacts an ordinance or adopts a resolution that complies with the requirements of sub. (2), the local government must determine the cost incurred in preparing the report specified in sub. (2) (c). As soon as practicable after the local government generates revenue from a facility specified in sub. (2) (intro.), the local government shall use the revenues to reimburse the treasury of the local government for the cost determined under this subsection.
History: 2003 a. 278, 327; 2007 a. 42.

Appendix Ten - DATCP

The Role of the Wisconsin Department of Agriculture, Transportation, and Consumer Protection (DATCP)

Overview of the Division of Trade and Consumer Protection

The Wisconsin Department of Agriculture, Trade and Consumer Protection is Wisconsin's primary consumer protection agency and has statutory and rulemaking authority over transactions between businesses and consumers. These statutes and rules serve as a framework that allows legitimate businesses to flourish, and provides consumers with confidence in the marketplace.

Consumer protection laws help ensure fair trade, competition, and the free flow of truthful information that help consumers make informed buying decisions. They are designed to prevent businesses that engage in fraud or specified unfair practices from gaining an advantage over competitors, and to protect consumers from fraud and deception.

Our highest priority is fighting fraudulent and deceptive practices that harm consumers and honest businesses.

Bureau of Consumer Protection

- Handles 100,000 new consumer complaints and inquiries every year
- Returns approximately $5 - $10 million on average to consumers annually
- Regulates unfair and deceptive business practices to protect millions of Wisconsin consumers every day

Protects consumers and honest competitors:

o Electronic communication services (telecommunications, cable TV, satellite TV, video services, Internet access services, etc.)

Has powerful fact-finding and compliance tools:

o Investigation and subpoena authority

https://datcp.wi.gov/Pages/About_Us/DTCPOverview.aspx

1913 The Legislature enacted the Fraudulent Advertising Law (ch. 510, Laws of 1913).
The Fraudulent Adverting Law, now known as the Fraudulent Representations Law, broadly prohibited deceptive advertising and sales practices. To this day, it is one of the state's most important consumer protection laws.

1921 The Legislature created a powerful new Department of Markets (ch. 571, Laws of 1921).
The impetus came from the agricultural sector, but the powers of the new department went far beyond agriculture:

• The new department was the state equivalent of the Federal Trade Commission (FTC).

• The department had sweeping authority to protect farmers, consumers, and honest competitors against unfair, deceptive, and anticompetitive business practices.

• Under Wisconsin's "Little FTC Act," the department was authorized to:

11

o Prohibit unfair business practices by industry-wide rules, or by orders directed to individual businesses. Violations were subject to strong penalties and a strong private remedy.

o Conduct investigations and hold investigative hearings.
o Subpoena witnesses and evidence.
• The new department had broad concurrent jurisdiction with other agencies:
o Monopolies and anti-trust (Attorney General)
o Deceptive advertising and sales practices (Treasury Agent)
*• The "Little FTC Act" became the cornerstone of Wisconsin's general trade regulation and consumer protection program**. Today, Wisconsin's law is still one of the most powerful state consumer protection laws in the nation***
https://datcp.wi.gov/Documents/HistoryofDATCPPrograms.pdf

Appendix Eleven - FCC

The Role of the Federal Communications Commission (FCC)

Mission Statement

1. Promoting competition, innovation, and investment in broadband services and facilities
2. Supporting the nation's economy by ensuring an appropriate competitive framework for the unfolding of the communications revolution
3. Developing and implementing regulatory programs
4. Conducting investigations and analyzing complaints

FCC email responses to complaints:
"The FCC's role in the complaint process is to facilitate a conversation between you and your provider."

Been there, done that. I have a stack of inconsequential and factually unsupported Charter lawyer letters to prove that, and you have a file full of my years of complaints.

I would add another responsibility.

5. To put the fear of government regulation into these exploitive monopolies

So that in my view the actual score card of wins and loses don't really count for that much. Monopoly behavior will change in places previously unseen, and you need to be on the right side of these issues for consumer/citizens; Net Neutrality, e-rate, orbital debris, AI ad disclosure, muni-networks, USF, are all important.

And remember this:

JOINT STATEMENT ON BROADBAND

- High-speed broadband is beginning to reshape every sector of our economy and many aspects of American life
- Broadband service can be an indispensable engine for unleashing innovation and investment, spurring job creation and economic growth, and ensuring our country's global competitiveness. Working to make sure that America has world-leading high-speed broadband networks—both wired and wireless—lies at the very core of the FCC's mission in the 21st Century
- Every American should have a meaningful opportunity to benefit from the broadband communications era—regardless of geography, race, economic status, disability, residence on tribal land, or degree of digital literacy
  https://docs.fcc.gov/public/attachments/FCC-10-42A1.pdf

(The role and responsibilities will be further articulated in full in a future novel published on leanpub.com, The Insider Goes Deep into Consumer Protection (A Journey NOT for the Faint of Heart)

Appendix Twelve - What are some Solutions?

Municipal Broadband

What Internet provider innovations have come from the increased competition among Internet providers with the Utopia Project in Utah?

The UTOPIA (Utah Telecommunication Open Infrastructure Agency) Project in Utah has played a key role in fostering innovation in Internet service provision, driven by the increased competition it introduced to the state's broadband market. UTOPIA is a municipal broadband network, which started in 2004 and aimed to provide high-speed fiber-optic Internet access to local residents and businesses. Its influence on the Internet service industry has sparked several notable innovations:

Faster Speeds and Lower Costs:

Increased Competition: By providing an open-access network, UTOPIA enabled multiple Internet service providers (ISPs) to offer services over the same fiber-optic infrastructure. This encouraged providers to offer competitive pricing and enhanced service offerings, such as faster speeds and more flexible service plans.

Gigabit Internet: UTOPIA's fiber-optic network allows for gigabit-speed Internet, and providers who use its infrastructure offer high-speed broadband, often at more affordable rates than traditional cable or DSL services.

Innovative Pricing Models:

Subscription Flexibility: UTOPIA's open-access model allowed users to choose from a variety of Internet service providers, each offering different pricing tiers and packages. This has encouraged more creative and competitive pricing structures, such as pay-as-you-go plans or more affordable, non-contract options that give consumers greater control over their service.

No Data Caps or Throttling: Providers on the UTOPIA network have often touted unlimited data usage with no throttling or data caps, which is a significant shift from traditional ISPs, which often impose limits or slow down speeds once certain usage thresholds are met.

Improved Customer Service and Satisfaction:

Focus on Consumer Needs: The competition spurred by UTOPIA has led many ISPs to focus more on customer service, offering better support, more transparency, and faster response times to maintain market share. This has been a direct contrast to the often less-responsive customer service of traditional cable or DSL companies.

Local Customer Service: Some ISPs leveraging the UTOPIA infrastructure have focused on offering more localized, community-centered customer service, helping to build stronger relationships with customers in the region.

Expanded Broadband Availability:

Rural Connectivity: UTOPIA's efforts have encouraged more infrastructure investment, particularly in underserved areas. Smaller and rural towns that were previously ignored by larger ISPs have gained access to faster and more affordable Internet. This has bridged the digital divide, promoting broader access to broadband services for education, work, and business.

Fiber Deployment: UTOPIA's extensive fiber-optic network encouraged private ISPs to accelerate their own fiber deployment efforts, further enhancing broadband availability and competition, which was essential for the growth of fiber-to-the-home (FTTH) technology.

Smarter Infrastructure Investments:

Open Access Infrastructure: UTOPIA's model of shared, open-access infrastructure has led other municipalities to explore similar models, driving innovation in how broadband networks can be built, managed, and shared. This model also encourages collaboration between public entities and private businesses to maximize the utility of broadband infrastructure.

Leveraging Existing Infrastructure: The project has promoted the idea of using existing municipal or publicly owned infrastructure (such as utility poles and conduits) to deploy broadband services, which has lowered costs for providers and sped up the rollout of new Internet access.

Alternative Services and Partnerships:

Smart City Initiatives: Some UTOPIA-connected areas have used the broadband infrastructure to support additional services such as smart city projects, including intelligent traffic management systems, improved public safety tools, and efficient energy grids. The availability of high-speed Internet allows local governments to deploy more advanced technologies that enhance the quality of life for residents.

Partnerships with Tech Companies: Increased competition from UTOPIA has also led to partnerships between ISPs and technology companies to deliver innovative services, including content delivery, cloud computing, and specialized Internet services (e.g., for gaming or remote work) on the fiber network.

In summary, the UTOPIA project has spurred significant innovation in Utah's Internet service market, fostering better speeds, pricing, service offerings, and even infrastructure deployment, all driven by the need for increased competition. It serves as a model for other areas seeking to enhance broadband access and stimulate local economies through improved digital connectivity.

Washington State Votes To End Restriction On Community Broadband (vice.com)

A report from Motherboard: *Washington State lawmakers have voted to kill telecom-industry backed restrictions that limit the reach of community broadband. The Public Broadband Act (HB1336) passed the state Senate with a 27-22 vote on Sunday, after passing the House with a vote of 60-37 last February. State Representative Drew Hansen applauded the bill's passage on Twitter, stating it "reverses decades of bad policy" and opens the door to better, cheaper broadband. "Washington was one of only 18 states that restricted local governments from serving the public by providing public broadband," Hansen told Motherboard. "My bill eliminates that restriction."*

In Washington, a twenty-one year old law let some local governments build their own broadband networks, but prohibited local utilities from delivering broadband to customers directly. Hansen, who was also the primary sponsor of the state's new net neutrality law, says his bill finally eliminates those unnecessary limits entirely. "The Public Broadband Act broadly authorizes all local governments to provide broadband to anyone -- people who are totally unserved, people who have some internet access but it's not affordable or reliable -- any people at all," Hansen told Motherboard. "Under the Public Broadband Act, Washington governments have completely unrestricted authority to provide broadband to the public."

Another US state repeals law that protected ISPs from municipal ...

May 24, 2024Minnesota this week eliminated two laws that made it harder for cities and towns to build their own **broadband** networks. The **state**-imposed **restrictions** were repealed in an omnibus commerce policy ...

Colorado Repeal Of Community Broadband Ban A Turning Point Decades In ...
Colorado **state** leaders have **voted to** eliminate long-criticized **state** barriers to municipal **broadband** networks. **Community broadband** advocates hope it will be a beacon for other **states** eager to bring more reliable and affordable high-speed Internet service to a market long dominated by monopoly

The State of State Preemption: Stalled - But Moving In More Competitive ...
Nov 1, 2024In 2021, Arkansas and Washington passed legislation significantly rolling back legislative barriers on publicly owned **broadband** networks. In 2023, Colorado rolled back a law that required communities to hold a referendum vote to opt out of a **state** ban on municipal **broadband**. That law

Municipal Broadband Remains Roadblocked In 16 States
May 14, 2024For decades, municipal **broadband** operations have been subject to a minefield of **restrictions** and barriers designed to make the prospect of establishing or maintaining a **community broadband** network costly, difficult, and unsustainable. The Biden administration initially pledged that

https://broadbandnow.com/report/municipal-broadband-roadblocks/
https://statescoop.com/report-municipal-broadband-environment-has-gotten-significantly-worse/
https://statescoop.com/more-than-20-states-still-restrict-municipal-broadband/

Appendix Thirteen - Conclusions

The Wisconsin Broadband maps are wrong, make the BEAD process flawed and destined for failure due mostly to a lack of imagination (And what to do about it)

In this century we have returned to the online service walled gardens and centralized controls of yesteryear with Amazon AWS, Google(Docs and Gmail), and Microsoft Azure, antithetic to the origins of the Internet and vision of the Internet elders, like Vannevar Bush, JCR Licklider, Lawrence Roberts, Vint Cert, Doug Engelbart, Ted Nelson, Tim Berners-Lee, Paul Baran, John Postel, Paul Baran, Leonard Kleinrock, Donald Davies, Robert Kahn, Bob Metcalf, and Tim Berners-Lee. We have now legalized and normalized the data harvesting vulture surveillance capitalism these new monopolies provide.

There are not any good reasons in my view that these parasitic and predatory overseers cannot be replaced by local libraries, municipalities, and non-profit agencies exercising local control for local residents and consumers, using local policies tied into the larger networks.

We have also now in fact returned to, a subsidized system, and allowed the monopolization of telecommunications much as it was prior to the breakup of AT&T in 1982.[1] Recent history shows that when AT&T was forced to share phone and DSL lines, this begat TDS, Frontier, and others offering the same services at lower prices. Competition? Imagine that!

Based on history, and in the view of many, it is critical to the future of our children, grandchildren as well as to our participatory democracy, that the following things happen:[2]

1. **Additional authorities be provided to the Public Services Commission (PSC) to further regulate telecommunications. Wisconsin municipalities and consumers need to lobby the Madison legislators to provide these authorities.[3] We must at all costs avoid the rampant fraud of the previous Federal pandemic era programs.**
2. **All fiber infrastructure must be shared (Charter, Comcast, AT&T, Frontier, TDS etc.) giving the consumer choices they do not have now and using a competitive market to determine pricing and services.[4] Public funding of Internet infrastructure and the simultaneous privatization of operator profits are not reflective of the invisible hand of the free market. There can be no prioritizing of traffic (fast private and slow public lanes) via DiffServ or differentiated services code point or DSCP. Net Neutrality, in its true sense, must prevail.**
3. **The relationship between municipalities and ISP's must change. These Federal BEAD funds are effectively corporate welfare. They are incentives to encourage investment in their very own (but heavily subsidized) infrastructure of dumb pipes. These ISP's don't actually _make_ anything, but just simply transport content created elsewhere.**

---

[1] https://en.wikipedia.org/wiki/Breakup_of_the_Bell_System

[2] The Book of Violations & Egregious Acts: Trillion Dollar Broadband Scandal by Bruce Kushnick (Author), David Rosen (Author) Format: Kindle Edition
DISS-CONNECTED: How America's Big Telecoms Stole Billions from the Public and Created the Digital Divide by David Rosen (Author), Bruce Kushnick (Author) Format: Kindle Edition
Telecom Book of Broken Promises.pdf by Bruce Kushnick (Author) https://newnetworks.com
$200 Billion Broadband Scandal.pdf by Bruce Kushnick (Author) https://newnetworks.com

[3] 196.504 Broadband expansion grant program; Broadband Forward! community certification.

[4] https://arstechnica.com/tech-policy/2023/11/canada-forces-large-fiber-isps-to-share-networks-with-small-competitors/

They are being encouraged by Federal tax monies to make these investments rather than engage is stock buybacks or pass revenues on as shareholder dividends or excessive CEO salaries. [5]

4. ISP advertised and billed Mbps service to customers must be metered and billed based on actual delivery to a meter (like municipal water, natural gas, and electricity). This does not mean data caps as Megabytes and Gigabytes delivered must NOT be measured or constrained in any way beyond ISP network operators managing their networks. This would be akin to measuring utility water pressure or voltage to your home, without which gallons per minute or kilowatt hours, or in this case Megabits, cannot be fully delivered to consumers.[6]

5. Testing of Mbps delivered must be done in a manner more consistent with actual consumer usage. Testing directly from the router firmware, as Cisco and perhaps others offer, bypasses any residential Wi-Fi issues, web browser engine speed variances (Chromium or Gecko), browser extension issues, browser tests are also reliant on browser timing calls, which can vary depending on the browser and device, antivirus interference, and software firewall issues. This direct router testing can run 24x7, because it is automated, can run hourly, and will not run when the network is in use, thereby providing the most accurate results. https://samknows.cdn.prismic.io/samknows/a773a0d4-5606-4d69-b2dd-5de724e31b7c_ConstantCare.pdf

To quote broadband expert Garland McCoy,President of the Technology Education Institute at Technology Education Institute https://alec.org/person/garland-t-mccoy/

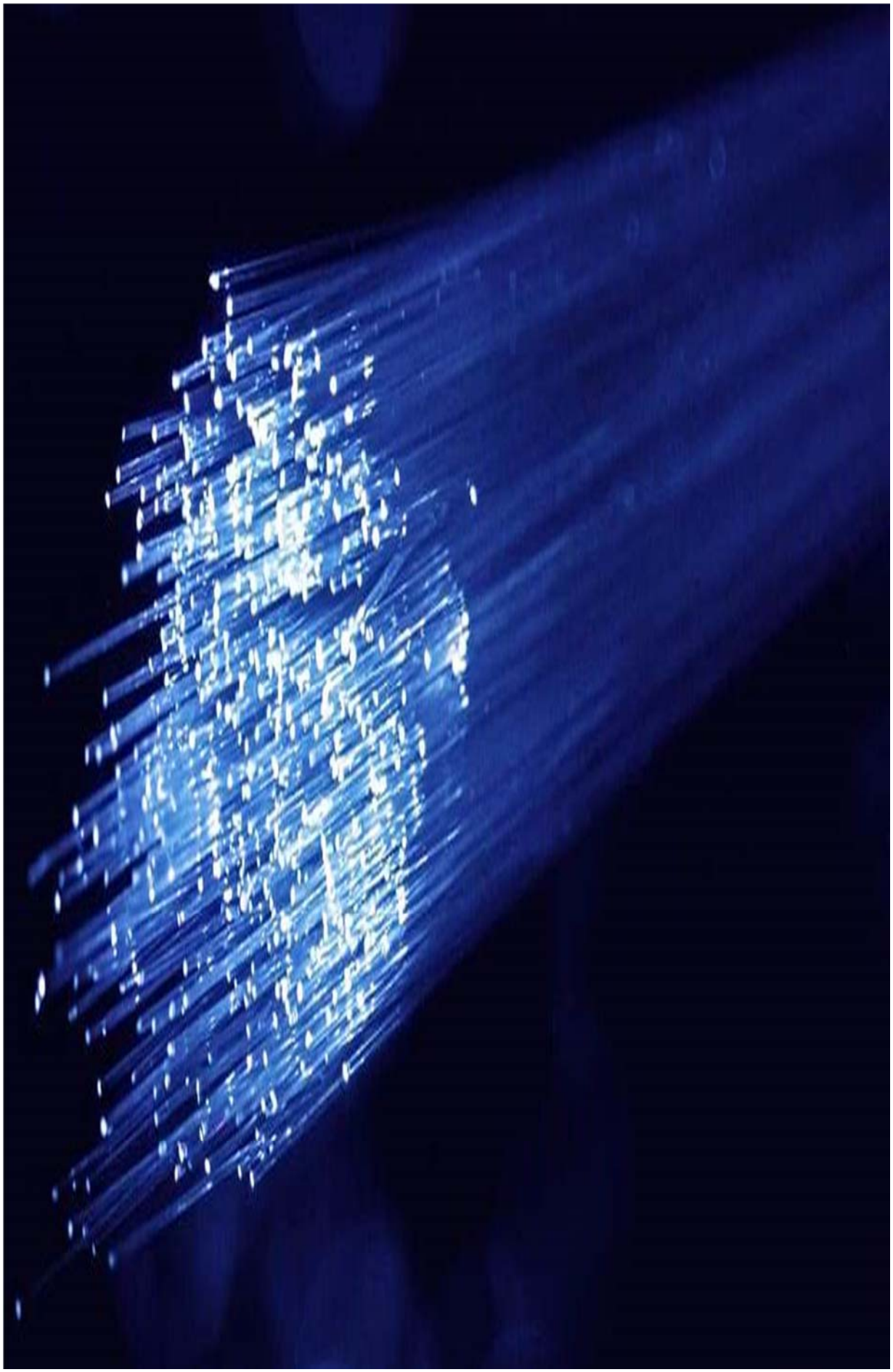
"Standards are needed for the measurement and testing of the "retail" broadband marketplace. FCC and BERC "Best Practices" testing is from the CPE to the ISPs IXP which best captures the complete users experience. An automated, standards based, methodology operated by an unaffiliated (this is important for trust) third party is needed. The methodology will generate trusted apple-to-apple data statewide . This can be done at scale (in the tens of millions) in short order with the probe ad delivered in the CPE and the target in IXPS. Filtering is minimized and everything is transparent and open source. This has the benefit helping reconcile the growing gap between state broadband maps and the FCC National Broadband Map."

6. **Municipalities must get involved in providing telecommunications services to its citizens, much as they have previously done with local electrical generation, local radio and TV stations, and local telephone companies.**[7] **Public assets must never be privatized. Municipalities must have visibility into local consumer data.(signups, speed tiers, and disconnects)**

---

[5] Following a proposal from Democrats that the federal government spend $80 billion funding the deployment of fast broadband — with upload/download speeds of 100Mbps — across underserved areas, AT&T is arguing that it's not worth the money because rural people should be happy with slower Internet service than cities get. "[T]here would be significant additional cost to deploy fiber to virtually every home and small business in the country, when at present there is no compelling evidence that those expenditures are justified over the service quality of a 50/10 or 100/20Mbps product," AT&T wrote in a blog post.
https://www.inverse.com/input/tech/att-doesnt-want-us-to-fund-fast-Internet-in-rural-areas

[6] https://www.samknows.com/products/constantcare

[7] Wisconsin Statute Annotated § 66.0422

The Insider Goes Deep into Broadband